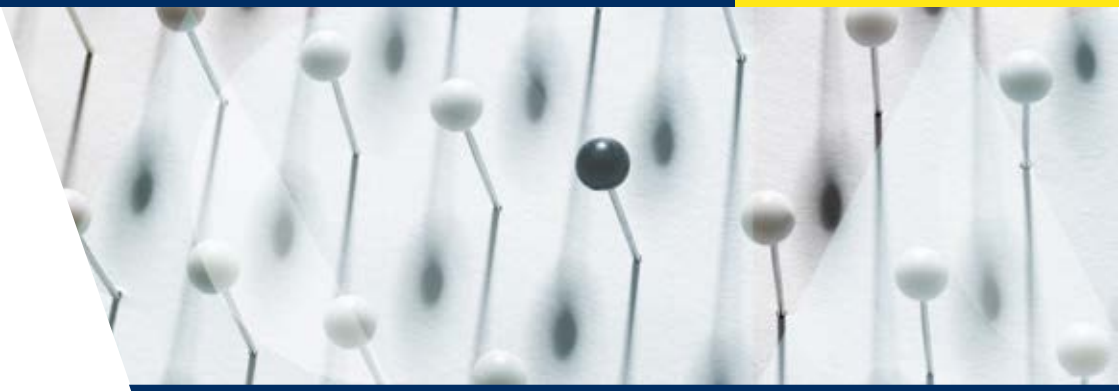
PRIRUČNIK



Priručnik o evropskom pravu zaštite podataka

Izdanje 2018.

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Rukopis ovog priručnika završen je u aprilu 2018.

Ažurirane verzije ubuduće će biti na raspolaganju na internet stranici Agencije Evropske unije za osnovna prava (FRA) na adresi fra.europa.eu, na internet stranici Saveta Evrope na adresi coe.int/dataprotection, na internet stranici Evropskog suda za ljudska prava na adresi echr.coe.int, u registru Case-Law (Sudska praksa), kao i na internet stranici Evropskog nadzornika za zaštitu podataka na adresi edps.europa.eu.

Fotografija (naslovnica i unutrašnjost): © iStockphoto

Ovaj dokument je preveden sa engleskog (*„Handbook on European data protection law - 2018 edition"*) od strane Evropske unije i Saveta Evrope. FRA ne snosi odgovornost za ovaj prevod.

Prevod ove publikacije je pripremljen uz finansijsku podršku Evropske unije i Saveta Evrope, kroz zajednički program „Horizontal Facility za Zapadni Balkan i Tursku, u okviru projekta „Zaštita slobode izražavanja i medija u Srbiji (PROFREX)".

Sadržaj je isključiva odgovornost autora i ni u kom slučaju ne predstavlja zvanične stavove Evropske unije ni Saveta Evrope.

Sufinansira Evropska unija

EVROPSKA UNIJA

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Sufinansira i sprovodi Savet Evrope

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Priručnik o evropskom pravu zaštite podataka

Izdanje 2018.

Predgovor

Naše društvo je sve više digitalizovano. Brzina tehnološkog razvoja i način obrade ličnih podataka svakodnevno utiču na svakog od nas na različite načine s obzirom na promene koje se odvijaju. Pravni okviri Evropske unije (EU) i Saveta Evrope kojima se obezbeđuje zaštita privatnosti i ličnih podataka nedavno su preispitani.

Evropa ima jednu od vodećih uloga u zaštiti podataka na svetskom nivou. Standardi zaštite podataka EU zasnivaju se na Konvenciji br. 108 Saveta Evrope, instrumentima EU – uključujući Opštu uredbu o zaštiti podataka i Direktivu o zaštiti podataka za policiju i tela krivičnog pravosuđa – kao i na odgovarajućoj sudskoj praksi Evropskog suda za ljudska prava i Suda pravde Evropske unije.

Reforme u području zaštite podataka koje su sproveli EU i Savet Evrope opsežne su i u nekim slučajevima složene, imaju širok raspon prednosti i utiču na pojedince i preduzeća. Cilj ovog priručnika je da podigne svest i doprinese boljem poznavanju propisa o zaštiti podataka, naročito među nespecijalizovanim pravnicima koji se u svom radu sreću sa problemima zaštite podataka.

Priručnik su izradili Agencija Evropske unije za osnovna prava (FRA), Savet Evrope (u saradnji sa Sekretarijatom Evropskog suda za ljudska prava) i Evropski nadzornik za zaštitu podataka. Njime se ažurira izdanje iz 2014. i pripada seriji pravnih priručnika koje su zajednički izradili FRA i Savet Evrope.

Želimo da zahvalimo telima za zaštitu podataka u Belgiji, Estoniji, Francuskoj, Gruziji, Irskoj, Italiji, Mađarskoj, Monaku, Švajcarskoj i Ujedinjenom Kraljevstvu za korisne povratne informacije o nacrtu priručnika. Takođe želimo da zahvalimo jedinici za zaštitu podataka Evropske komisije i njenoj jedinici za međunarodne prenose i zaštitu podataka. Zahvaljujemo Sudu pravde Evropske unije za podršku u vidu dokumentacije pružene tokom pripreme ovog priručnika.

Christos Giakoumopoulos	**Giovanni Buttarelli**	**Michael O'Flaherty**
Generalni direktor za ljudska prava i vladavinu prava Saveta Evrope	Evropski nadzornik za zaštitu podataka	Direktor Agencije Evropske unije za osnovna prava

Sadržaj

Skraćenice i akronimi

BCR	Obavezujuće korporativno pravilo
CCTV	Televizija zatvorenog kruga
CETS	Zbirka ugovora Saveta Evrope
CIS	Carinski informacioni sistem
SE	Savet Evrope
CRM	Upravljanje odnosima s kupcima
C-ŠIS	Centralni šengenski informacioni sistem
DPA	Nadležno telo za zaštitu podataka
SZP	Službenik za zaštitu podataka
ENH	Evropski nalog za hapšenje
EDPS	Evropski nadzornik za zaštitu podataka
EFSA	Evropska agencija za bezbednost hrane
EFTA	Evropsko udruženje slobodne trgovine
EEP	Evropski ekonomski prostor
EKLJP	Evropska konvencija o ljudskim pravima
ENISA	Agencija Evropske unije za mrežnu i informacionu bezbednost
ENU	Europolova nacionalna jedinica
EOZP	Evropski odbor za zaštitu podataka
KEJT	Kancelarija evropskog javnog tužioca
ESLJP	Evropski sud za ljudska prava
ESMA	Evropsko nadzorno telo za vrednosne papire i tržišta kapitala
eTEN	Transevropske telekomunikacione mreže
EU	Evropska unija
eu-LISA	Agencija Evropske unije za operativno upravljanje opsežnim informacionim sistemima
EuroPriSe	Evropski pečat za zaštitu podataka
EZ	Evropska zajednica
FRA	Agencija Evropske unije za osnovna prava

OUZP	Opšta uredba o zaštiti podataka
GPS	Globalni sistem pozicioniranja
MPGPP	Međunarodni pakt o građanskim i političkim pravima
IKT	Informacione i komunikacione tehnologije
PUS	Pružalac usluga interneta
ZNT	Zajedničko nadzorno telo
Konvencija br. 108	Konvencija o zaštiti pojedinaca pri automatskoj obradi ličnih podataka (Savet Evrope). Protokol o izmeni (CETS br. 223) Konvencije br. 108 („modernizovana Konvencija br. 108") doneo je Odbor ministara Saveta Evrope prilikom 128. zasedanja održanog u Helsingoru u Danskoj (od 17. do 18. maja 2018). Upućivanja na „modernizovanu Konvenciju br. 108" odnose se na Konvenciju izmenjenu Protokolom CETS br. 223.
N-ŠIS	Nacionalni šengenski informacioni sistem
NVO	Nevladina organizacija
OECD	Organizacija za ekonomsku saradnju i razvoj
PIN	Lični identifikacioni broj
EIP	Evidencija imena putnika
Povelja	Povelja Evropske unije o osnovnim pravima
KGN	Koordinaciona grupa za nadzor
SEPA	Jedinstvena zona plaćanja u evrima
SPEU	Sud pravde Evropske unije (pre decembra 2009. poznat kao Evropski sud, ECJ)
ŠIS	Šengenski informacioni sistem
SL	Službeni list
SWIFT	Društvo za svetsku međubankovnu finansijsku telekomunikaciju
ODLJP	Opšta deklaracija o ljudskim pravima
UEU	Ugovor o Evropskoj uniji
UFEU	Ugovor o funkcionisanju Evropske unije
UN	Ujedinjene nacije
VIS	Vizni informacioni sistem

Kako se koristi ovaj priručnik

Ovaj priručnik daje pregled pravnih standarda u vezi sa zaštitom podataka koje su utvrdili Evropska unija (EU) i Savet Evrope (SE). Osmišljen je kao pomoć stručnjacima koji nisu specijalizovani u oblasti zaštite podataka, uključujući advokate, sudije i druge radnike u pravosuđu, kao i zaposlene u drugim telima kao što su nevladine organizacije (NVO), koji se mogu sresti sa pravnim pitanjima u vezi sa zaštitom podataka.

Priručnik služi kao prva referentna tačka o relevantnom pravu Unije, Evropskoj konvenciji o ljudskim pravima (EKLJP) kao i Konvenciji Saveta Evrope o zaštiti pojedinaca pri automatskoj obradi ličnih podataka (Konvencija br. 108) i drugim instrumentima Saveta Europe.

Svako poglavlje započinje tablicom u kojoj su navedeni propisi važni za teme iz pripadajućeg poglavlja. Tablice obuhvataju i pravo Saveta Evrope i pravo Unije i sadrže odabranu sudsku praksu Evropskog suda za ljudska prava (ESLJP) i Suda pravde Evropske unije (SPEU). Zatim su relevantni zakoni tih dvaju evropskih sistema predstavljeni jedan za drugim prema primenjivosti na svaku od tema. Na taj način čitaoci mogu da saznaju po čemu su ta dva pravna sistema slična, a po čemu se razlikuju. To bi čitaocima trebalo da pomogne i u pronalaženju ključnih informacija koje se odnose na njihove slučajeve, naročito ako podležu samo pravu Saveta Evrope. U određenim poglavljima, u kojima je to korisno za sažet prikaz sadržaja, redosled tema u tablicama može se donekle razlikovati od teksta samog poglavlja. U priručniku se takođe pruža kratak pregled okvira Ujedinjenih nacija.

Pravnici u državama koje nisu članice Unije, ali su članice Saveta Evrope i ugovorne strane Evropske konvencije o ljudskim pravima i Konvencije br. 108, mogu da pogledaju informacije koje se odnose na njihove države direktno u odeljcima koji se odnose na Savet Evrope. Pravnici u državama koje nisu članice Unije moraju imati na umu i da se od donošenja Opšte uredbe Evropske unije o zaštiti podataka propisi EU o zaštiti podataka primenjuju na organizacije i druge subjekte koji nemaju sedište u EU ako obrađuju lične podatke i pružaju proizvode i usluge ispitanicima u Uniji ili prate njihovo ponašanje.

Pravnici u državama članicama Unije moraće da pogledaju oba odeljka, jer su za te države obavezujuća oba pravna poretka. Vredi napomenuti da su uporedo sprovedene reforme i modernizacija propisa o zaštiti podataka u Evropi, u okviru Saveta Evrope (modernizovana Konvencija br. 108 izmenjena Protokolom CETS br. 223) i

u okviru EU (donošenje Opšte uredbe o zaštiti podataka i Direktive 2016/680/EU). Donosioci propisa u oba pravna sistema preduzeli su sve mere kako bi obezbedili doslednost i usklađenost tih dvaju pravnih okvira. Reformama je zato postignuta veća usklađenost zakonodavstva o zaštiti podataka Saveta Evrope i EU. Za osobe kojima su potrebne podrobnije informacije o određenoj temi predviđen je popis detaljnijih materijala u odeljku pod nazivom „Dodatna literatura". Informacije o odredbama Konvencije br. 108 i njenog dodatnog Protokola iz 2001. godine, koje se primenjuju do stupanja na snagu Protokola o izmeni, dostupne su u izdanju priručnika iz 2014. godine.

Pravo Saveta Evrope predstavljeno je kratkim upućivanjima na odabrane predmete Evropskog suda za ljudska prava (ESLJP). Oni su odabrani iz velikog broja presuda i odluka tog suda u predmetima koji se odnose na zaštitu podataka.

Relevantno pravo EU obuhvata donesene zakonodavne mere, relevantne odredbe ugovora i Povelju Evropske unije o osnovnim pravima, kako su protumačeni u sudskoj praksi SPEU. Usto, priručnik donosi mišljenja i smernice koje je donela Radna grupa iz člana 29., savetodavno telo koje je na osnovu Direktive o zaštiti podataka dobilo zadatak pružanja stručnih saveta državama članicama EU, a koje je od 25. maja 2018. zamenio Evropski odbor za zaštitu podataka (EOZP). Mišljenja Evropskog nadzornika za zaštitu podataka takođe pružaju značajan uvid u tumačenje prava Unije, pa su stoga uvršćena u ovaj priručnik.

Predmetima opisanim ili citiranim u ovom priručniku daju se primeri iz važnog skupa sudske prakse ESLJP-a i SEU-a. Smernice na kraju priručnika služe kao pomoć čitaocima u traženju sudske prakse na internetu. Prikazana sudska praksa SPEU odnosi se na prethodnu Direktivu o zaštiti podataka. Međutim, tumačenja SPEU-a i dalje su primenjiva na pripadajuća prava i obaveze utvrđene Opštom uredbom o zaštiti podataka.

Zatim, u okvirima tekstova sa plavom pozadinom prikazane su praktične ilustracije s hipotetičkim scenarijima. Njima se dodatno objašnjava primena evropskih propisa o zaštiti podataka u praksi, naročito u slučajevima nepostojanja relevantne sudske prakse ESLJP-a ili SPEU. U ostalim tekstnim okvirima koji imaju sivu pozadinu navode se primeri preuzeti iz izvora koji ne pripadaju sudskoj praksi ESLJP-a i SPEU, kao što su zakonodavstvo i mišljenja Radne grupe iz člana 29.

U uvodnom delu priručnika ukratko je opisana uloga dvaju pravnih sistema koja su uspostavljena Evropskom konvencijom o ljudskim pravima i pravom Unije (poglavlje 1). Poglavlja od 2 do 10 obuhvataju sledeće teme:

- terminologija u vezi sa zaštitom podataka
- glavna načela evropskog prava zaštite podataka
- propisi evropskog prava zaštite podataka
- nezavisni nadzor
- prava ispitanika i njihovo sprovođenje
- prekogranični prenosi ličnih podataka
- zaštita podataka u kontekstu policije i krivičnog pravosuđa
- ostali evropski propisi o zaštiti podataka u određenim zonama
- savremeni izazovi zaštite ličnih podataka.

1

Kontekst i pozadina evropskog zakonodavstva o zaštiti podataka

EU	Obuhvaćena pitanja	Savet Evrope
Pravo na zaštitu podataka		
Ugovor o funkcionisanju Evropske unije, član 16. Povelja Evropske unije o osnovnim pravima (Povelja), član 8. (pravo na zaštitu ličnih podataka) Direktiva 95/46/EZ o zaštiti pojedinaca u vezi sa obradom ličnih podataka i o slobodnom protoku takvih podataka (Direktiva o zaštiti podataka), SL 1995 L 281 (na snazi do maja 2018) Okvirna odluka Saveta 2008/977/PUP o zaštiti ličnih podataka obrađenih u okviru policijske i pravosudne saradnje u krivičnim stvarima, SL 2008 L 350 (na snazi do maja 2018) Uredba (EU) 2016/679 o zaštiti pojedinaca u vezi s obradom ličnih podataka i o slobodnom kretanju takvih podataka kao i o stavljanju van snage Direktive 95/46/EZ (Opšta uredba o zaštiti podataka), SL 2016 L 119 Direktiva (EU) 2016/680 o zaštiti pojedinaca u vezi s obradom ličnih podataka od strane nadležnih tela u svrhe sprečavanja, istrage, otkrivanja ili gonjenja krivičnih dela ili izvršavanja krivičnih sankcija i o slobodnom kretanju takvih podataka kao i o stavljanju van snage Okvirne odluke Saveta 2008/977/PUP (zaštita podataka za policiju i tela		EKLJP, član 8. (pravo na poštovanje privatnog i porodičnog života, doma i prepiske) Modernizovana konvencija o zaštiti pojedinaca pri automatskoj obradi ličnih podataka, (modernizovana Konvencija br. 108)

EU	Obuhvaćena pitanja	Savet Evrope
krivičnog prava), SL 2016 L 119 Direktiva 2002/58/EZ o obradi ličnih podataka i zaštiti privatnosti u zoni elektronskih komunikacija (Direktiva o privatnosti i elektronskim komunikacijama), SL 2002 L 201 Uredba (EZ) br. 45/2001 o zaštiti pojedinaca u vezi s obradom ličnih podataka u institucijama i telima Zajednice i o slobodnom kretanju takvih podataka (Uredba o zaštiti podataka u institucijama Evropske unije), SL 2001 L 8		
Ograničenje prava na zaštitu ličnih podataka		
Povelja, član 52. stav 1. Opšta uredba o zaštiti podataka, član 23. SPEU, spojeni predmeti C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen* [VV], 2010.		EKLJP, član 8. stav 2. Modernizovana konvencija br. 108, član 11 ESLJP, *S. i Marper protiv Ujedinjenog Kraljevstva* [VV], br. 30562/04 i 30566/04, 2008.
Uravnotežavanje prava		
SPEU, spojeni predmeti C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen* [VV], 2010.	**Uopšteno**	
SPEU, C-73/07, *Tietosuojavaltuutettu protiv Satakunnan Markkinapörssi Oy i Satamedia Oy* [VV], 2008. SPEU, C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González* [VV], 2014.	**Sloboda izražavanja**	ESLJP, *Axel Springer AG protiv Nemačke* [VV], br. 39954/08, 2012. ESLJP, *Mosley protiv Ujedinjenog Kraljevstva*, br. 48009/08, 2011. ESLJP, *Bohlen protiv Nemačke*, br. 53495/09, 2015.
SPEU, C-28/08 P, *Evropska komisija protiv The Bavarian Lager Co. Ltd* [VV], 2010. SPEU, C-615/13P, *ClientEarth i Pesticide Action Network Europe (PAN Europe) protiv Evropske agencije za sigurnost hrane (EFSA) i Evropske komisije (EFSA)*, 2015.	**Pristup dokumentima**	ESLJP, *Magyar Helsinki Bizottság protiv Mađarske* [VV], br. 18030/11, 2016.
Opšta uredba o zaštiti podataka, član 90	**Poslovna tajna**	ESLJP, *Pruteanu protiv Rumunije*, br. 30181/05, 2015.
Opšta uredba o zaštiti podataka, član 91	**Sloboda veroispovesti ili uverenja**	

EU	Obuhvaćena pitanja	Savet Evrope
	Sloboda umetnosti i nauke	ESLJP, *Vereinigung bildender Künstler protiv Austrije*, br. 68354/01, 2007.
SPEU, C-275/06, *Productores de Música de España (Promusicae) protiv Telefónica de España SAU* [VV], 2008.	Zaštita svojine	
SPEU, C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González* [VV], 2014. SPEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce protiv Salvatorea Mannija*, 2017.	Ekonomska prava	

1.1. Pravo na zaštitu ličnih podataka

Ključne tačke

- Prema članu 8. Evropske konvencije o ljudskim pravima, pravo na zaštitu pojedinca u pogledu obrade ličnih podataka je deo prava na poštovanje privatnog i porodičnog života, doma i prepiske.
- Konvencija br. 108 Saveta Evrope prvi je i trenutno jedini međunarodni pravno obavezujući instrument koji se bavi zaštitom podataka. Konvencija je modernizovana i dopunjena donošenjem Protokola o izmeni CETS br. 223.
- Prema pravu EU, zaštita podataka priznata je kao zasebno osnovno pravo. To je potvrđeno članom 16. Ugovora o funkcionisanju Evropske unije i članom 8. Povelje EU o osnovnim pravima.
- Prema pravu EU, zaštita podataka prvi put je regulisana 1995. godine Direktivom o zaštiti podataka.
- Uzimajući u obzir brz tehnološki razvoj, EU je 2016. godine donela nove zakone kako bi propise o zaštiti podataka prilagodila digitalnom dobu. Opšta uredba o zaštiti podataka stupila je na snagu u maju 2018. i njome je Direktiva o zaštiti podataka stavljena van snage.
- Uz Opštu uredbu o zaštiti podataka, EU je usvojila propise o obradi ličnih podataka koju sprovode državna tela u svrhu sprovođenja zakonodavstva. Direktivom (EU) 2016/680 utvrđuju se pravila i načela zaštite podataka kojima se uređuje obrada ličnih podataka u svrhe sprečavanja, istrage, otkrivanja ili gonjenja krivičnih dela ili izvršavanja krivičnih sankcija.

1.1.1. Pravo na poštovanje privatnog života i pravo na zaštitu ličnih podataka: kratak uvod

Iako su usko povezana, pravo na poštovanje privatnog života i pravo na zaštitu ličnih podataka zasebna su prava. Pravo na privatnost, koje se u evropskom zakonodavstvu naziva pravom na poštovanje privatnog života, uvedeno je u međunarodno zakonodavstvo o ljudskim pravima Opštom deklaracijom o ljudskim pravima (ODLJP) iz 1948. godine kao jedno od osnovnih zaštićenih ljudskih prava. Ubrzo nakon donošenja ODLJP, Evropa je potvrdila to pravo Evropskom konvencijom o ljudskim pravima (EKLJP), sporazumom sastavljenim 1950. koji je pravno obavezujuć za njegove ugovorne strane. EKLJP-om se određuje da svaka osoba ima pravo na poštovanje svog privatnog i porodičnog života, doma i prepiske. Javnim telima zabranjuje se mešanje u to pravo, osim u slučajevima u kojima je to u skladu sa zakonom, kada se time nastoji da se ostvari važan i legitiman javni interes ili je to nužno u demokratskom društvu.

ODLJP i EKLJP doneseni su mnogo pre razvoja računara i interneta kao i pojave informatičkog društva. To je donelo znatne prednosti pojedincima i društvu i poboljšalo kvalitet života, efikasnost i produktivnost. S druge strane, pojavili su se i novi rizici za pravo na poštovanje privatnog života. Kao odgovor na potrebu za posebnim propisima kojima se uređuje prikupljanje i upotreba ličnih podataka, uveden je nov koncept privatnosti, koji se u nekim nadležnostima naziva „informaciona privatnost", a u nekima „pravo na informaciono samoodređenje"[1]. Taj koncept je doveo do razvoja posebnih zakonskih propisa kojima se obezbeđuje zaštita ličnih podataka.

Zaštita podataka u Evropi započela je 1970-ih usvajanjem propisa, u pojedinim državama, radi kontrole obrade ličnih podataka koju sprovode javna tela i velike kompanije[2]. Posle toga uspostavljeni su instrumenti za zaštitu podataka na nivou

1 Savezni ustavni sud Nemačke potvrdio je pravo na informaciono samoodređenje presudom u predmetu *Volkszählungsurteil* iz 1983. godine, BVerfGE Bd. 65, S. 1ff. Sud je zaključio da informaciono samoodređenje proizlazi iz osnovnog prava na poštovanje ličnosti, koje je zaštićeno nemačkim Ustavom. ESLJP je presudom iz 2017. potvrdio da se članom 8. EKLJP „garantuje pravo na jedan oblik informacionog samoodređenja". Videti ESLJP, *Satakunnan Markkinapörssi Oy i Satamedia Oy protiv Finske* [VV], br. 931/13, 27. juna 2017, stav 137.

2 Nemačka savezna država Hesen donela je 1970. godine prvi zakon o zaštiti podataka koji se primenjivao samo u toj državi. Švedska je 1973. donela prvi domaći zakon o zaštiti podataka u svetu. Do kraja 1980-ih nekoliko evropskih država (Francuska, Nemačka, Holandija i Ujedinjeno Kraljevstvo) je takođe donelo zakone o zaštiti podataka.

Evrope[3], pa se s vremenom zaštita podataka razvila u posebnu vrednost koja nije obuhvaćena pravom na poštovanje privatnog života. U pravnom poretku EU zaštita podataka priznata je kao osnovno pravo odvojeno od osnovnog prava na poštovanje privatnog života. Zbog takvog razdvajanja se postavlja pitanje odnosa i razlika između tih prava.

Pravo na poštovanje privatnog života i pravo na zaštitu ličnih podataka usko su povezani. Ovim pravima se nastoji da se zaštite slične vrednosti, odnosno autonomija i ljudsko dostojanstvo pojedinaca, obezbeđivanjem lične sfere u kojoj mogu slobodno da razvijaju svoje ličnosti, razmišljaju i oblikuju sopstvena mišljenja. Ona su stoga nužan preduslov za ostvarivanje drugih osnovnih sloboda, kao što su sloboda izražavanja, sloboda mirnog okupljanja i udruživanja i sloboda veroispovesti.

Ta dva prava razlikuju se prema formulaciji i oblasti primene. Pravo na poštovanje privatnog života uključuje opštu zabranu mešanja, osim u određenim slučajevima postojanja javnog interesa koji bi mogao da opravda takvo mešanje. Zaštita ličnih podataka smatra se savremenim i aktivnim pravom[4] kojim se uspostavlja sistem provera i ravnoteže kako bi se pojedinci zaštitili prilikom svake obrade njihovih podataka. Obrada mora biti u skladu s osnovnim elementima zaštite ličnih podataka, prvenstveno nezavisnim nadzorom i poštovanjem prava ispitanika[5].

Članom 8. Povelje EU o osnovnim pravima (Povelja) ne samo što se potvrđuje pravo na zaštitu ličnih podataka, već se objašnjavaju i osnovne vrednosti u vezi sa tim pravom. Njime se utvrđuje da obrada ličnih podataka mora biti pravična, mora se sprovoditi u utvrđene svrhe i zasnivati se na pristanku osobe o kojoj je reč ili legitimnoj osnovi utvrđenoj zakonom. Pojedinci moraju imati pravo na pristup svojim ličnim podacima i na njihovo ispravljanje, a poštovanje tog prava mora da podleže kontroli nezavisnog tela.

3 Konvencija Saveta Evrope o zaštiti pojedinaca pri automatskoj obradi ličnih podataka (Konvencija br. 108) usvojena je 1981. godine. EU je 1995. donela prvi sveobuhvatni instrument zaštite podataka: Direktivu 95/46/EZ o zaštiti pojedinaca u vezi sa obradom ličnih podataka i o slobodnom protoku takvih podataka.

4 Opšta pravozastupnica Šarpston navela je da predmet obuhvata dva zasebna prava: „klasično" pravo na zaštitu privatnosti i „savremenije" pravo na zaštitu podataka. Videti SPEU, spojeni predmeti C-92/09 i C-93/02, *Volker und Markus Schecke GbR protiv Land Hessen*, *Opinion of Advocate General Sharpston* (Mišljenje opšte pravozastupnice Šarpston), 17. juna 2010, stav 71.

5 Hustinx, P., Govori i članci EDPS-a, *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, srpanj 2013.

Pravo na zaštitu ličnih podataka primenjuje se prilikom svake obrade ličnih podataka, pa je zato šire od prava na poštovanje privatnog života. Svaki postupak obrade ličnih podataka podleže odgovarajućoj zaštiti. Zaštita podataka obuhvata razne vrste ličnih podataka i obrade podataka, nezavisno od njihovog odnosa i uticaja na privatnost. Obradom ličnih podataka takođe se može kršiti pravo na privatni život, kao što je vidivo u primerima u nastavku. Međutim, nije potrebno dokazati povredu prava na privatni život kako bi se primenila pravila zaštite podataka.

Pravo na privatnost odnosi se na situacije u kojima je ugrožen privatni interes ili „privatni život" pojedinca. Kao što će biti pokazano u ovom priručniku, koncept „privatnog života" široko se tumači u sudskoj praksi tako da obuhvata intimne situacije, osetljive ili poverljive informacije, informacije koje bi mogle da dovedu naškode tome kako javnost doživljava određenog pojedinca, pa čak i aspekte nečijeg profesionalnog života i ponašanja u javnosti. Međutim, procena postojanja mešanja u „privatni život" zavisi od konteksta i okolnosti svakog pojedinačnog slučaja.

S druge strane, svaka radnja koja uključuje obradu ličnih podataka može da bude obuhvaćena oblašću primene propisa o zaštiti podataka i uslovljavati sprovođenje prava na zaštitu ličnih podataka. Na primer, ako poslodavac beleži informacije o imenima i naknadama zaposlenih, samo beleženje tih informacija ne može se smatrati mešanjem u privatni život. To bi se, međutim, moglo smatrati mešanjem ako bi poslodavac prenosio lične podatke zaposlenih trećim licima. Poslodavci se u svakom slučaju moraju pridržavati propisa o zaštiti podataka, jer beleženje podataka o zaposlenima predstavlja obradu podataka.

Primer: U predmetu *Digital Rights Ireland*[6] SPEU je trebalo da donese odluku o valjanosti Direktive 2006/24/EZ u kontekstu osnovnih prava na zaštitu ličnih podataka i poštovanje privatnog života, koja su potvrđena Poveljom EU o osnovnim pravima. Direktivom se pružaocima javno dostupnih elektronskih komunikacionih usluga ili javnih komunikacionih mreža nalagalo zadržavanje komunikacionih podataka građana najviše dve godine, kako bi se obezbedilo da podaci budu dostupni u svrhe sprečavanja, istrage i gonjenja teških krivičnih dela. Ta mera se odnosila samo na meta-podatke, podatke o lokaciji i podatke neophodne za identifikaciju pretplatnika ili korisnika. Nije se primenjivala na sadržaj elektronskih komunikacija.

6 SPEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr.* i *Kärntner Landesregierung i dr.* [VV], 8. aprila 2014.

SPEU je zaključio da Direktiva predstavlja mešanje u osnovno pravo na zaštitu ličnih podataka „s obzirom na to da predviđa obradu ličnih podataka"[7]. Takođe, SPEU je zaključio da se Direktiva upliće u pravo na poštovanje privatnog života[8]. Uzeti zajedno, lični podaci zadržani u skladu sa Direktivom, kojima mogu pristupiti nadležna tela, mogu da omoguće „donošenje vrlo preciznih zaključaka o privatnom životu osoba čiji su podaci zadržani, kao što su svakodnevne navike, mesta trajnih ili privremenih boravaka, dnevno ili drugo kretanje, obavljane aktivnosti, društveni odnosi i društvene sredine koje su te osobe posećivale"[9]. Mešanje u ta dva prava bilo je široko i naročito ozbiljno.

SPEU je proglasio Direktivu 2006/24/EZ nevažećom, zaključivši da je, iako je njome nastojao da se ostvari legitiman cilj, mešanje u prava na zaštitu ličnih podataka i privatni život bilo ozbiljno i nije bilo ograničeno na ono što je strogo nužno.

1.1.2. Međunarodni pravni okvir: Ujedinjene nacije

U okviru Ujedinjenih nacija zaštita ličnih podataka nije prepoznata kao osnovno pravo, iako je pravo na privatnost davno uspostavljeno osnovno pravo u međunarodnom pravnom poretku. Član 12. Opšte deklaracije o ljudskim pravima (ODLJP) o poštovanju privatnog i porodičnog života[10] prvi je slučaj u kojem je međunarodnim instrumentom utvrđeno pravo pojedinca na zaštitu njegove privatne sfere od mešanja drugih, naročito države. Iako je reč o neobavezujućoj deklaraciji, ODLJP ima značajan status osnovnog instrumenta međunarodnog prava o ljudskim pravima te je uticao na razvoj drugih instrumenata ljudskih prava u Evropi. Međunarodni pakt o građanskim i političkim pravima (MPGPP) stupio je na snagu 1976. U njemu se navodi da niko ne sme da bude podvrgnut samovoljnom ili nezakonitom mešanju u njegov privatni život, porodicu ili prepisku, ni nezakonitim napadima na njegovu čast ili ugled. MPGPP je međunarodni sporazum kojim se njegovih 169 ugovornica obavezuje na poštovanje i garanciju sprovođenja građanskih prava pojedinaca, uključujući privatnost.

7 *Ibid.*, stav 36.

8 *Ibid.*, stavovi od 32. do 35.

9 *Ibid.*, stavi 27.

10 Ujedinjene nacije (UN), Universal Declaration of Human Rights (UDHR), 10. decembra 1948.

Počev od 2013. Ujedinjene nacije donele su dve rezolucije u vezi sa pitanjem privatnosti pod nazivom „pravo na privatnost u digitalnom dobu"[11] kao odgovor na razvoj novih tehnologija i razotkrivanje slučajeva masovnog nadzora u nekim državama (objava informacija Edvarda Snoudena). U njima je iznesena snažna osuda masovnog nadzora i istaknut efekat koji takav nadzor može da ima na osnovna prava na privatnost i slobodu izražavanja, kao i na funkcionisanje dinamičnog, demokratskog društva. Iako rezolucije nisu pravno obavezujuće, podstakle su važnu međunarodnu političku raspravu na visokom nivou na temu privatnosti, novih tehnologija i nadzora. Takođe su dovele do imenovanja Specijalnog izvestioca UN za pitanja prava na privatnost, s ovlašćenjem za unapređenje i zaštitu tog prava. Specijalni zadaci izvestioca uključuju prikupljanje informacija o domaćim praksama i iskustvima u vezi sa privatnošću i izazovima koji proizlaze iz novih tehnologija, razmenu i promovisanje najboljih praksi kao i utvrđivanje mogućih prepreka.

Ranije su rezolucije bile usmerene na negativne efekte masovnog nadzora i odgovornost vlada da ograniče ovlašćenja obaveštajnih službi, dok novije rezolucije odražavaju ključnu novu pojavu u raspravi o privatnosti u Ujedinjenim nacijama[12]. U rezolucijama usvojenim 2016. i 2017. godine potvrđuje se potreba za ograničenjem ovlašćenja obaveštajnih agencija i osuđuje masovni nadzor. Međutim, u njima se takođe izričito navodi da „sve veća mogućnost preduzeća da prikupljaju, obrađuju i upotrebljavaju lične podatke može predstavljati rizik za uživanje prava na privatnost u digitalnom dobu". Stoga se uz odgovornost državnih tela u rezolucijama ističe i obaveza privatnog sektora da poštuje ljudska prava, pa se kompanije podstiču na obaveštavanje korisnika o prikupljanju, upotrebi, deljenju i zadržavanju ličnih podataka i na donošenje transparentnih pravila o obradi podataka.

1.1.3. Evropska konvencija o ljudskim pravima

Savet Evrope osnovan je posle Drugog svetskog rata kako bi okupio države Evrope radi promocije vladavine prava, demokratije, ljudskih prava i društvenog razvoja. U tu svrhu je Savet 1950. doneo Evropsku konvenciju o ljudskim pravima (EKLJP), koja je stupila na snagu 1953. godine.

11 Vidi UN, Generalna skupština, Resolution on the right to privacy in the digital age, A/RES/68/167, New York, 18. decembra 2013; i UN, Generalna skupština, Revised draft resolution on the right to privacy in the digital age, A/C.3/69/L.26/Rev. 1, New York, 19. novembra 2014.

12 UN, Generalna skupština, Revised draft resolution on the right to privacy in the digital age, A/C.3/71/L.39/Rev. 1, New York, 16. novembra 2016.; UN, Savet za ljudska prava, The right to privacy in the digital age, A/HRC/34/L.7/Rev. 1, 22. marta 2017.

Ugovorne strane Konvencije imaju međunarodnu obavezu njenog poštovanja. Sve države članice Saveta Evrope ugradile su ili sprovele EKLJP u svojim nacionalnim zakonodavstvima, što ih obavezuje na poštovanje odredbi Konvencije. Ugovorne strane moraju da poštuju prava navedena u Konvenciji prilikom izvršavanja bilo kakve aktivnosti ili ovlašćenja. To uključuje radnje preduzete zbog nacionalne bezbednosti. Istorijske presude Evropskog suda za ljudska prava (ESLJP) odnosile su se na državne aktivnosti u osetljivim oblastima zakonodavstva i prakse u vezi sa nacionalnom bezbednošću[13]. Sud je bez oklevanja potvrdio da radnje nadzora predstavljaju mešanje u poštovanje privatnog života[14].

Kako bi se obezbedilo da ugovorne strane poštuju svoje obaveze preuzete EKLJP--om, u Strazburu, u Francuskoj, osnovan je 1959. godine Evropski sud za ljudska prava (ESLJP). Taj sud obezbeđuje da države poštuju obaveze preuzete Konvencijom i razmatra prigovore pojedinaca, grupa pojedinaca, nevladinih organizacija ili pravnih lica zbog navodnog kršenja Konvencije. ESLJP može da razmatra i međudržavne predmete koje je jedna država članica Saveta Evrope (ili više njih) podnela protiv druge države članice.

Savet Evrope je 2018. brojao 47 država članica, od kojih su 28 i države članice Evropske unije. Podnosilac predstavke koji se obraća ESLJP-u ne mora da bude državljanin ugovorne strane, ali navodna kršenja moraju da se dogode na području u nadležnosti jedne od ugovornih strana.

Pravo na zaštitu ličnih podataka je deo prava zaštićenih članom 8. EKLJP-a kojim se garantuje pravo na poštovanje privatnog i porodičnog života, doma i prepiske i propisuju uslovi u kojima su dopuštena ograničenja tog prava[15].

ESLJP je razmatrao mnoge situacije u vezi sa pitanjima zaštite podataka. One uključuju presretanje komunikacije,[16] razne oblike nadzora koje vrše i privatni i javni sek-

13 Na primer, vidi sledeće: ESLJP, *Klass i drugi protiv Nemačke*, br. 5029/71, 6. septembra 1978.; ESLJP, *Rotaru protiv Rumunije* [VV], br. 28341/95, 4. maja 2000. i ESLJP, *Szabó i Vissy protiv Mađarske*, br. 37138/14, 12. januara 2016.

14 *Ibid*.

15 Savet Evrope, European Convention on Human Rights, CETS br. 005, 1950.

16 Na primer, vidi sledeće: ESLJP, *Malone protiv Ujedinjenog Kraljevstva*, br. 8691/79, 2. avgusta 1984.; ESLJP, *Copland protiv Ujedinjenog Kraljevstva*, br. 62617/00, 3. aprila 2007, ili ESLJP, *Mustafa Sezgin Tanrıkulu protiv Turske*, br. 27473/06, 18. jula 2017.

tor[17] i zaštitu od čuvanja ličnih podataka javnih tela[18]. Poštovanje privatnog života nije apsolutno pravo, jer se ostvarivanjem prava na privatnost mogu ugroziti druga prava, kao što su sloboda izražavanja i pristupa informacijama i obrnuto. Stoga ESLJP nastoji da postigne ravnotežu između različitih prava o kojima je reč. Sud je pojasnio da se članom 8. EKLJP-a države obavezuju ne samo na uzdržavanje od svih radnji kojima bi mogle da prekrše to pravo iz Konvencije, već i da se u određenim okolnostima pozitivno obavezuju na aktivno unapređivanje efikasnog poštovanja privatnog i porodičnog života[19]. Mnogi od tih slučajeva podrobno su opisani u odgovarajućim poglavljima.

1.1.4. Konvencija br. 108 Saveta Evrope

Od pojave informacione tehnologije 1960-ih godina, rasla je potreba za podrobnijim propisima kojima bi se zaštitili lični podaci pojedinaca. Sredinom 70-ih godina Savet ministara Saveta Evrope usvojio je više rezolucija o zaštiti ličnih podataka pozivajući se na član 8. EKLJP-a[20]. Konvencija o zaštiti pojedinaca pri automatskoj obradi ličnih podataka (Konvencija br. 108)[21] otvorena je za potpisivanje 1981. Konvencija br. 108 bila je i ostala jedini pravno obavezujući međunarodni instrument u oblasti zaštite podataka.

Konvencija br. 108 primenjuje se na svaku obradu podataka u privatnom i u javnom sektoru, uključujući obradu u sudstvu i u policiji. Konvencija štiti pojedince od zloupotreba prilikom obrade ličnih podataka i istovremeno zahteva regulisanje prekograničnog prenosa ličnih podataka. U pogledu obrade ličnih podataka, načela iz Konvencije naročito se tiču pravičnog i zakonitog prikupljanja i automatske obrade podataka u određene legitimne svrhe. To znači da podaci ne smeju da se upotrebljavaju u druge neprikladne svrhe i da ne smeju da se zadržavaju duže nego što je to potrebno. Ta načela se odnose i na kvalitet podataka: oni u prvom redu moraju da budu prikladni, relevantni, tačni i ne smeju da budu suvišni (srazmernost).

---

17 Na primer, vidi sledeće: ESLJP, *Klass i drugi protiv Nemačke,* br. 5029/71, 6. septembra 1978.; ESLJP, *Uzun protiv Nemačke*, br. 35623/05, 2. septembra 2010.

18 Na primer, vidi sledeće: ESLJP, *Roman Zakharov protiv Rusije*, br. 47143/06, 4. decembra 2015.; ESLJP, *Szabó i Vissy protiv Mađarske*, br. 37138/14, 12. januara 2016.

19 Na primer, vidi sledeće: ESLJP, *I. protiv Finske*, br. 20511/03, 17. jula 2008.; ESLJP, *K. U. protiv Finske*, br. 2872/02, 2. decembra 2008.

20 Savet Evrope, Savet ministara (1973.), Rezolucija (73) 22 o zaštiti privatnosti pojedinaca *vis-à-vis* elektronskih banki podataka u privatnom sektoru, 26. septembra 1973.; Savet Evrope, Savet ministara (1974), Rezolucija (74) 29 o zaštiti privatnosti pojedinaca *vis-à-vis* elektronskih banaka podataka u javnom sektoru, 20. septembra 1974.

21 Savet Evrope, Konvencija o zaštiti pojedinaca pri automatskoj obradi ličnih podataka, CETS br. 108, 1981.

Osim garancija u pogledu obrade ličnih podataka i obaveza bezbednosti podataka, Konvencijom se, u odsustvu prikladnih pravnih mera zaštite, zabranjuje obrada „osetljivih" podataka, kao što su rasa, političko opredeljenje, zdravlje, vera, seksualni život ili kaznena evidencija pojedinca.

Konvencijom se takođe štiti pravo pojedinca na obaveštenost o tome da li se podaci o njemu čuvaju, te, ako je to neophodno, ispravljanje takvih podataka. Ograničenja prava utvrđenih Konvencijom moguća su samo kada su posredi važniji interesi, kao što je bezbednost ili odbrana države. Osim što se Konvencijom omogućava slobodan prenos ličnih podataka među ugovornim stranama Konvencije, njome se takođe nameću određena ograničenja prenosa u države čije pravno uređenje ne pruža isti nivo zaštite.

Treba napomenuti da je Konvencija br. 108 obavezujuća za države koje su je ratifikovale. Konvencija ne podleže sudskom nadzoru ESLJP-a, ali se razmatra u okviru sudske prakse ESLJP-a u kontekstu člana 8. EKLJP-a. Tokom godina ESLJP je presuđivao da je zaštita ličnih podataka važan deo prava na poštovanje privatnog života (član 8.) i vodio se načelima Konvencije br. 108 u odlučivanju o postojanju mešanja u to osnovno pravo[22].

Kako bi nastavio da razvija opšta načela i pravila iz Konvencije br. 108, Savet ministara Saveta Evrope usvojio je nekoliko pravno neobavezujućih preporuka. Te preporuke su doprinele razvoju zakonodavstva o zaštiti podataka u Evropi. Na primer, godinama je jedini instrument, koji je davao smernice o upotrebi ličnih podataka u sektoru policije u Evropi, bila Preporuka o policiji[23]. Načela Preporuke, kao što su načini čuvanja baza podataka i potreba sprovođenja jasnih pravila o osobama kojima je dopušten pristup tim bazama, dodatno su razvijena i ugrađena u naknadno zakonodavstvo EU[24]. Novije preporuke usmerene su na rešavanje izazova digitalnog doba, na primer u vezi s obradom podataka u kontekstu zapošljavanja (vidi poglavlje 9).

Sve države članice EU su ratifikovale Konvenciju br. 108. Godine 1999. predložene su izmene Konvencije br. 108 kako bi se omogućilo da EU postane ugovorna strana,

22 Na primer, vidi sledeće: ESLJP, *Z. protiv Finske*, br. 22009/93, 25. februara 1997.

23 Savet Evrope, Savet ministara (1987), Preporuka Rec(87)15 državama članicama o upotrebi ličnih podataka u policijskom sektoru, Strazbur, 17. septembra 1987.

24 Direktiva 95/46/EZ Evropskog parlamenta i Saveta od 24. oktobra 1995. o zaštiti pojedinaca u vezi sa obradom ličnih podataka i o slobodnom protoku takvih podataka, SL L 281, 23. novembra 1995.

ali nikada nisu stupile na snagu[25]. Dodatni protokol uz Konvenciju br. 108 usvojen je 2001. godine. Njime su uvedene odredbe o prekograničnom prenosu podataka u zemlje koje nisu ugovorne strane Konvencije, tzv. trećim zemljama, te o obaveznom uspostavljanju nacionalnih tela nadležnih za zaštitu podataka[26].

Konvenciji br. 108 mogu pristupiti države koje nisu članice Saveta Evrope. Potencijal Konvencije kao univerzalnog standarda i njen otvoren karakter služe kao osnova unapređenja zaštite podataka na globalnom nivou. Do sada je 51 zemlja potpisala Konvenciju br. 108. One uključuju sve države članice Saveta Evrope (47 zemalja), Urugvaj, prvu neevropsku zemlju koja je Konvenciji pristupila u avgustu 2013. godine, kao i Mauricijus, Senegal i Tunis, koji su pristupili 2016. i 2017.

Konvencija je nedavno podvrgnuta postupku modernizacije. Javno savetovanje sprovedeno 2011. godine potvrdilo je dva glavna cilja tog postupka: veću zaštitu privatnosti u digitalnom okruženju i jačanje mehanizma praćenja sprovođenja Konvencije. Postupak modernizacije bio je usmeren na te ciljeve, a dovršen je donošenjem protokola o izmeni Konvencije br. 108 (Protokol CETS br. 223). Postupak se sprovodio istovremeno s drugim reformama međunarodnih instrumenata za zaštitu podataka, kao i reformom propisa EU o zaštiti podataka pokrenutom 2012. godine. Donosioci propisa na nivou Saveta Evrope i EU preduzeli su sve mere kako bi obezbedili doslednost i usklađenost tih dvaju pravnih okvira. Modernizacijom je očuvan opšti i fleksibilni karakter Konvencije i potvrđen njen potencijal kao univerzalnog pravnog instrumenta u oblasti zaštite podataka. Njome se potvrđuju i stabilizuju važna načela i daju nova prava pojedincima, a istovremeno se povećavaju i obezbeđuju odgovornosti tela koja obrađuju lične podatke. Na primer, osobe čiji se lični podaci obrađuju imaju pravo da saznaju razloge za takvu obradu podataka i pravo na prigovor na takvu obradu. Kako bi se suzbila povećana upotreba izrade profila na mreži, Konvencijom se takođe utvrđuje pravo pojedinca da ne bude predmet odluka koje se zasnivaju isključivo na automatizovanoj obradi, bez uzimanja u obzir njegovog mišljenja. Stvarno sprovođenje propisa o zaštiti podataka, koje obavljaju nezavisna nadzorna tela u zemljama ugovornim stranama smatra se ključnom za sprovođenje Konvencije u praksi. Zbog toga se u modernizovanoj Konvenciji ističe

25 Savet Evrope, Izmene Konvencije o zaštiti pojedinaca pri automatskoj obradi ličnih podataka (ETS br. 108), koje je doneo Savet ministara u Strazburu 15. juna 1999.

26 Savet Evrope, Dodatni protokol uz Konvenciju o zaštiti pojedinaca pri automatskoj obradi ličnih podataka, koji se tiče nadzornih tela i prekograničnih prenosa podataka, CETS br. 181, 2001. Modernizacijom Konvencije br. 108 ovaj protokol je prestao da se primenjuje jer su njegove odredbe izmenjene i ugrađene u modernizovanu Konvenciju br. 108.

potreba za davanjem efikasnih ovlašćenja i funkcija nadzornim telima kao i za stvarnom nezavisnošću u obavljanju njihovog zadatka.

1.1.5. Zakonodavstvo Evropske unije o zaštiti podataka

Pravo EU sastoji se od primarnog i sekundarnog prava. Ugovore, odnosno Ugovor o Evropskoj uniji (UEU) i Ugovor o funkcionisanju Evropske unije (UFEU), ratifikovale su sve države članice EU i oni zajedno čine „primarno pravo Unije". Uredbe, direktive i odluke EU donele su institucije EU koje su za to ovlašćene ugovorima i one zajedno čine „sekundarno pravo EU".

Zaštita podataka u primarnom pravu EU

U izvornim ugovorima Evropskih zajednica nisu spominjana ni ljudska prava, niti njihova zaštita, budući da je Evropska ekonomska zajednica prvobitno zamišljena kao regionalna organizacija usmerena ka ekonomskoj integraciji i uspostavljanju zajedničkog tržišta. Osnovno načelo na kojem počivaju osnivanje i razvoj Evropskih zajednica, koje je podjednako aktuelno i danas, jeste načelo dodele. Prema tom načelu, EU deluje isključivo unutar ograničenja nadležnosti koje mu dodele države članice, što je utvrđeno ugovorima o EU. Za razliku od Saveta Evrope, u ugovorima o EU ne utvrđuje se nikakva izričita nadležnost u pogledu osnovnih prava.

Međutim, budući da su se pred SPEU pojavljivali predmeti o navodnim povredama ljudskih prava unutar oblasti primene prava EU, SPEU je pružio važna tumačenja ugovora. Kako bi garantovao zaštitu pojedincima, ugradio je osnovna prava u takozvane opšta načela evropskog prava. Prema Sudu pravde Evropske unije, ta opšta načela odražavaju način na koji su ljudska prava zaštićena u domaćim ustavima i ugovorima o ljudskim pravima, a naročito u EKLJP-u. SPEU je naveo da će obezbediti usklađenost prava EU sa tim načelima.

Uviđajući da njene politike mogu da utiču na ljudska prava i nastojeći da izgradi „bliskiji" odnos sa svojim državljanima, Evropska unija proglasila je Povelju Evropske unije o osnovnim pravima (Povelja) 2000. godine. Povelja obuhvata ceo niz građanskih, političkih, ekonomskih i socijalnih prava evropskih građana sintetišući ustavne tradicije i međunarodne obaveze zajedničke državama članicama. Prava sadržana u Povelji dele se u šest kategorija: dostojanstvo, slobode, jednakost, solidarnost, prava građana i pravda.

Povelja je isprva bila samo politički dokument, ali stupanjem na snagu Ugovora iz Lisabona 1. decembra 2009., postala je pravno obavezujuća[27] kao primarno pravo EU (videti član 6. stav 1. Ugovora o Evropskoj uniji)[28]. Odredbe Povelje namenjene su institucijama i telima EU, obavezujući ih da poštuju prava navedena u njoj pri izvršavanju svojih obaveza. Odredbe Povelje obavezujuće su i za države članice prilikom sprovođenja prava EU.

Ne samo da se Poveljom garantuje poštovanje privatnog i porodičnog života (član 7.), nego se utvrđuje i pravo na zaštitu ličnih podataka (član 8.). Poveljom se nivo takve zaštite izričito podiže na nivo zaštite osnovnih prava u okviru prava EU. Institucije i tela EU moraju garantovati i poštovati to pravo, kao i države članice pri sprovođenju prava EU (član 51. Povelje). Formulisan nekoliko godina posle Direktive o zaštiti podataka, član 8. Povelje treba shvatiti tako da otelotvoruje postojeće zakonodavstvo o zaštiti podataka Evropske unije. Stoga, osim što se u članu 8. stav 1. Povelje izričito spominje pravo na zaštitu podataka, u članu 8. stav 2. upućuje se i na ključna načela zaštite podataka. Na kraju, članom 8. stav 3. Povelje propisuje se da nezavisno telo sprovodi kontrolu sprovođenja tih načela.

Donošenje Ugovora iz Lisabona je prekretnica u razvoju prava zaštite podataka, ne samo zbog uzdizanja Povelje na nivo pravno obavezujućeg dokumenta primarnog prava, nego i zbog pružanja prava na zaštitu ličnih podataka. To pravo se izričito navodi u članu 16. UFEU, u delu ugovora posvećenom opštim načelima EU. Član 16. takođe čini novu pravnu osnovu kojom se EU dodeljuje nadležnost za donošenje propisa u oblasti zaštite podataka. To je važno jer su se propisi EU o zaštiti podataka, naročito Direktiva o zaštiti podataka, prvobitno zasnivali na pravnoj osnovi unutrašnjeg tržišta i na potrebi usklađivanja nacionalnih zakona kako slobodno kretanje podataka u EU ne bi bilo ograničeno. Član 16. UFEU sada daje nezavisnu pravnu osnovu za savremen, sveobuhvatan pristup zaštiti podataka, koji obuhvata sva pitanja u nadležnosti EU, uključujući policijsku i pravosudnu saradnju u krivičnim stvarima. Članom 16. UFEU takođe se potvrđuje da usklađenost s propisima o zaštiti podataka koji su doneseni u skladu s njim mora da podleže kontroli nezavisnih nadzornih tela. Član 16. poslužio je kao pravna osnova za sprovođenje sveobuhvatne reforme propisa o zaštiti podataka 2016. godine, odnosno Opšte uredbe o zaštiti podataka i Direktive o zaštiti podataka za policiju i tela krivičnog pravosuđa (vidi u nastavku).

27 EU (2012.), Povelja Evropske unije o osnovnim pravima, SL 2012 C 326.

28 Videti pročišćeni tekst Evropskih zajednica (2012.), Ugovor o Evropskoj uniji, SL 2012 C 326; i Evropskih zajednica (2012.), UFEU, SL 2012 C 326.

Opšta uredba o zaštiti podataka (GDPR)

Od 1995. do maja 2018. godine, glavni pravni instrument EU u vezi sa zaštitom podataka bila je Direktiva 95/46/EZ Evropskog parlamenta i Saveta od 24. oktobra 1995. o zaštiti pojedinaca u vezi sa obradom ličnih podataka i o slobodnom protoku takvih podataka (Direktiva o zaštiti podataka)[29]. Donesena je 1995. godine, u vreme kada je nekoliko država članica već donelo domaće zakone o zaštiti podataka,[30] a proizašla je iz potrebe za usklađivanjem tih zakona kako bi se obezbedio visok nivo zaštite i slobodan protok ličnih podatka među različitim državama članicama. Preduslov za slobodno kretanje robe, kapitala, usluga i ljudi na unutrašnjem tržištu bio je slobodan prenos podataka koji se nije mogao ostvariti bez pouzdanog i ujednačeno visokog nivoa zaštite podataka u državama članicama.

U Direktivi o zaštiti podataka odražavala je, a često i proširivala, načela zaštite podataka koji su već bili obuhvaćeni domaćim zakonima i Konvencijom br. 108. U Direktivi je ostavljena mogućnost dodavanja instrumenata zaštite, koja je predviđena članom 11. Konvencije br. 108. Uvođenje nezavisne kontrole u direktivi, kao instrumenta za bolju usklađenost s propisima o zaštiti podataka, pokazalo se važnim doprinosom delotvornosti evropskog prava zaštite podataka. Stoga je taj instrument 2001. godine ugrađen u pravo Saveta Evrope Dodatnim protokolom uz Konvenciju br. 108. To pokazuje usku povezanost i međusoban pozitivan uticaj dvaju instrumenata kroz godine.

Direktivom o zaštiti podataka uspostavljen je detaljan i sveobuhvatan sistem zaštite podataka u EU. Međutim, prema pravnom sistemu EU, direktive se ne primenjuju direktno već se moraju preneti u domaće zakone država članica. Države članice pritom imaju diskreciono pravo u prenošenju odredaba direktive. Iako je Direktivom nastojalo da se osigura potpuno usklađivanje[31] (i potpuna zaštita), u praksi se ona različito prenosila u pojedinim državama članicama. To je dovelo do postojanja različitih propisa o zaštiti podataka u EU i različitog tumačenja definicija i pravila u

29 Direktiva 95/46/EZ Evropskog parlamenta i Saveta od 24. oktobra 1995. o zaštiti pojedinaca u vezi s obradom ličnih podataka i o slobodnom protoku takvih podataka, SL 1995 L 281.

30 Nemačka savezna država Hesen donela je 1970. prvi zakon o zaštiti podataka u svetu, koji se primenjivao samo u toj državi. Švedska je 1973. donela zakon *Datalagen*, Nemačka je 1976. donela *Bundesdatenschutzgestez*, a Francuska je 1977. donela *Loi relatif à l'informatique, aux fichiers et aux libertés*. Ujedinjeno Kraljevstvo donelo je Zakon o zaštiti podataka 1984. (engl. *Data Protection Act*), a Holandija je 1989. donela *Wet Persoonregistraties*.

31 SPEU, spojeni predmeti C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) protiv Administración del Estado*, 24. novembra 2011, stav 29.

domaćim zakonima. Isto tako, nivoi sprovođenja i težina sankcija razlikovale su se među državama članicama. Konačno, od izrade nacrta Direktive sredinom 1990-ih došlo je do znatnih promena informacionih tehnologija. Svi ti razlozi podstakli su reformu zakonodavstva o zaštiti podataka u EU.

Reforma je dovela do donošenja Opšte uredbe o zaštiti podataka u aprilu 2016. godine, posle više godina intenzivnih rasprava. Rasprave o potrebi za modernizacijom propisa o zaštiti podataka u EU započele su 2009. godine, kada je Komisija pokrenula javno savetovanje o budućem pravnom okviru za osnovno pravo na zaštitu ličnih podataka. Komisija je objavila predlog uredbe u januaru 2012. godine, čime je započet dug zakonodavni postupak pregovora između Evropskog parlamenta i Saveta Evropske unije. Nakon usvajanja, Opšta uredba o zaštiti podataka omogućila je dvogodišnji prelazni period. U potpunosti je počela da se primenjuje od 25. maja 2018. godine, kada je van snage stavljena Direktiva o zaštiti podataka.

Donošenjem Opšte uredbe o zaštiti podataka 2016. modernizovano je zakonodavstvo EU o zaštiti podataka i time omogućena zaštita osnovnih prava u kontekstu ekonomskih i društvenih izazova digitalnog doba. GDPR-om se čuvaju i razvijaju osnovna načela i prava ispitanika koja su utvrđena Direktivom o zaštiti podataka. Usto, Uredbom su uvedene nove obaveze prema kojima organizacije moraju da sprovode tehničku i integrisanu zaštitu podataka, imenuju službenika za zaštitu podataka u određenim okolnostima, poštuju novo pravo na prenosivost podataka i pridržavaju se načela odgovornosti. U skladu sa pravom EU, uredbe su direktno primenjive, što znači da nije potrebno sprovođenje na domaćem nivou. Opšta uredba o zaštiti podataka zato daje jedinstveni skup pravila o zaštiti podataka na nivou EU. Time se stvaraju dosledna pravila o zaštiti podataka za celu EU i uspostavlja okruženje pravne bezbednosti od kojeg mogu imati koristi privredni subjekti i pojedinci kao „ispitanici".

Međutim, iako je Opšta uredba o zaštiti podataka direktno primenjiva, od država članica očekuje se da izmene svoje postojeće nacionalno zakonodavstvo o zaštiti podataka radi potpunog usklađivanja sa Uredbom, uz određena diskreciona prava koja se odnose na posebne odredbe iz uvodne izjave 10. Osnovna pravila i načela utvrđena Uredbom, kao i moćna prava koja se njome dodeljuju pojedincima, čine veliki deo ovog priručnika i prikazana su u narednim poglavljima. Uredba uključuje sveobuhvatna pravila u vezi sa teritorijalnom oblašću primene. Ona se primenjuje na preduzeća osnovana u EU i na rukovaoce podacima i obrađivače podataka koji nemaju prebivalište u EU, a koji pružaju proizvode ili usluge subjektima podataka (ispitanicima) u EU ili kontrolišu njihovo ponašanje. Budući da nekoliko stranih tehnoloških preduzeća ima značajan udeo na evropskom tržištu i milione potrošača u

EU, primena propisa EU o zaštiti podataka na te organizacije važna je za obezbeđivanje zaštite pojedinaca i ravnopravnih uslova poslovanja.

Zaštita podataka u policijskim stvarima – Direktiva 2016/680

Direktiva o zaštiti podataka koja je stavljena van snage pružala je sveobuhvatan sistem zaštite podataka. Taj sistem je dodatno proširen donošenjem Opšte uredbe o zaštiti podataka. Iako je nekadašnja Direktiva o zaštiti podataka bila sveobuhvatna, njena oblast primene bila je ograničena na aktivnosti koje pripadaju unutrašnjem tržištu kao i aktivnosti javnih organa koji nisu policijski. Zato je bilo potrebno donošenje posebnih instrumenata radi postizanja potrebne jasnoće i ravnoteže između zaštite podataka i drugih legitimnih interesa, kao i radi suočavanja s izazovima koji su posebno relevantni za određene sektore. To se odnosi na propise kojima se uređuje obrada ličnih podataka koju obavljaju organi reda/policijski organi.

Prvi pravni instrument EU kojim je uređeno ovo pitanje bila je Okvirna odluka Saveta 2008/977/PUP o zaštiti ličnih podataka obrađenih u okviru policijske i pravosudne saradnje u krivičnim stvarima. Odredbe Odluke primenjivane su se samo na policijske i pravosudne podatke koji su razmenjivani među državama članicama. Domaća obrada ličnih podataka koju obavljaju organi reda nije bila obuhvaćena njenom oblašću primene.

To je ispravljeno Direktivom 2016/680 o zaštiti pojedinaca u vezi s obradom ličnih podataka od strane nadležnih tela u svrhe sprečavanja, istrage, otkrivanja ili gonjenja krivičnih dela ili izvršavanja krivičnih sankcija i o slobodnom kretanju takvih podataka,[32] koja se naziva Direktivom o zaštiti podataka za policiju i tela krivičnog pravosuđa. Direktiva je donesena istovremeno s Opštom uredbom o zaštiti podataka. Njome je van snage stavljena Okvirna odluka 2008/977/PUP i uspostavljen sveobuhvatan sistem zaštite ličnih podataka u kontekstu rada policije/organa reda, a istovremeno su prepoznate posebnosti obrade podataka u vezi sa javnom bezbednošću. Dok se Opštom uredbom o zaštiti podataka utvrđuju opšta pravila za zaštitu pojedinaca u pogledu obrade njihovih ličnih podataka i obezbeđuje slobodan protoka takvih podataka unutar EU, Direktivom se utvrđuju posebna pravila za zaštitu podataka u oblastima pravosudne saradnje u krivičnim stvarima i policijske saradnje. Direktiva 2016/680 primenjivaće se na svaki slučaj u kojem nadležno telo

32 Direktiva (EU) 2016/680 Evropskog parlamenta i Saveta od 27. aprila 2016. o zaštiti pojedinaca u vezi s obradom ličnih podataka od strane nadležnih tela u svrhe sprečavanja, istrage, otkrivanja ili gonjenja krivičnih dela ili izvršavanja krivičnih sankcija i o slobodnom kretanju takvih podataka, SL L 119, 4. maja 2016.

obrađuje lične podatke u svrhu sprečavanja, istrage, otkrivanja ili gonjenja krivičnih dela. Kada nadležna tela obrađuju lične podatke u svrhe pored prethodno spomenutih, primenjivaće se opšti sistem opšte uredbe o zaštiti podataka. Za razliku od propisa koji joj je prethodio (Okvirna odluka Saveta 2008/977/PUP), oblast primene Direktive 2016/680 proširuje se na domaću obradu ličnih podataka koju obavljaju policijski organi/organi reda i nije ograničeno na razmenu takvih podataka među državama članicama. Usto, Direktivom se nastoji uspostavljanje ravnoteže između prava pojedinaca i legitimnih ciljeva obrade u bezbednosne svrhe.

U tu svrhu, u Direktivi se potvrđuju pravo na zaštitu ličnih podataka i osnovna načela koji bi trebalo da obuhvataju obradu podataka, koji su usko povezani s pravilima i načelima utvrđenim u Opštoj uredbi o zaštiti podataka. Prava pojedinaca i obaveze koje su propisane rukovaocima podacima, na primer u vezi sa bezbednošću podataka, tehničkom i integrisanom zaštitom podataka i obaveštavanjem u slučaju povrede podataka, slični su pravima i obavezama iz Opšte uredbe o zaštiti podataka. U Direktivi se takođe nastoji da se razmotre i reše novi, ozbiljni tehnološki izazovi koji mogu da imaju posebno težak uticaj na pojedince, kao što su metode izrade profila koje upotrebljavaju organi reda/policijski organi. U načelu, mora se zabraniti donošenje odluka isključivo na osnovu automatizovane obrade podataka, uključujući izradu profila[33]. Ono se isto tako ne sme zasnivati ni na osetljivim podacima. Za takva načela mogu da važe određeni izuzeci utvrđeni u Direktivi. Takođe, takva obrada ne sme da dovede do diskriminacije bilo koje osobe[34].

Direktiva takođe sadrži odredbe kojima se obezbeđuje odgovornost rukovalaca podacima. Oni moraju da imenuju službenika za zaštitu podataka koji će nadgledati usklađenost s propisima o zaštiti podataka, obaveštavati i savetovati to telo i zaposlene koji izvršavaju svoje obaveze obrade podataka i sarađivati s nadzornim telom. Obrada ličnih podataka u sektoru policije i krivičnog pravosuđa sada podleže kontroli nezavisnih nadzornih tela. I opšti pravni sistem zaštite podataka i poseban sistem zaštite podataka organa reda/policije i u krivičnim stvarima moraju u istoj meri da budu usklađeni sa zahtevima Povelje EU o osnovnim pravima.

Posebni sistem obrade podataka u kontekstu policije i pravosudne saradnje, uspostavljen Direktivom o zaštiti podataka za policiju i tela krivičnog pravosuđa, detaljno je opisan u poglavlju 8.

33 Direktiva o zaštiti podataka za policiju i tela krivičnog pravosuđa, član 11. stav 1.

34 *Ibid*., član 11. st. 2. i 3.

Direktiva o privatnosti i elektronskim komunikacijama

Utvrđivanje posebnih propisa za zaštitu podataka smatralo se potrebnim i u oblasti elektronskih komunikacija. Zbog razvoja interneta, fiksne i mobilne telefonije, bilo je važno obezbediti poštovanje prava korisnika na privatnost i poverljivost. Direktivom 2002/58/EZ[35] o obradi ličnih podataka i zaštiti privatnosti u oblasti elektronskih komunikacija (Direktiva o privatnosti i elektronskim komunikacijama) utvrđuju se pravila o bezbednosti ličnih podataka u tim mrežama, obaveštavanju u slučaju povrede ličnih podataka i poverljivosti komunikacija.

Kad je reč o bezbednosti, pružaoci elektronskih komunikacionih usluga moraju, između ostalog, obezbediti da pristup ličnim podacima bude ograničen isključivo na ovlašćena lica i preduzeti mere za sprečavanje uništavanja, gubitka ili nehotičnog oštećenja ličnih podataka[36]. Ako postoji poseban rizik od povrede bezbednosti javnih komunikacionih mreža, operatori moraju da obaveste pretplatnike o tom riziku[37]. Ako dođe do povrede bezbednosti uprkos preduzetim bezbednosnim merama, operatori moraju da obaveste nadležno nacionalno telo, koje ima zadatak da primeni i sprovede Direktivu, o slučaju povrede ličnih podataka. Operatori ponekad moraju da obaveste i pojedince o povredi ličnih podataka, na primer u slučaju kada bi takva povreda mogla negativno da utiče na njihove lične podatke ili privatnost[38]. Za očuvanje poverljivosti komunikacija potrebno je u načelu zabraniti slušanje, prisluškivanje, čuvanje ili bilo koji oblik nadzora ili presretanja komunikacija i metapodataka. Direktivom se takođe zabranjuju neželjene komunikacije (koje se često nazivaju „spam"), osim ako korisnici daju pristanak za to, a ona sadrži i pravila o čuvanju „kolačića" na računarima i drugim uređajima. Ove ključne negativne obaveze jasno upućuju na to da je poverljivost komunikacija snažno povezana sa zaštitom prava na poštovanje privatnog života sadržanog u članu 7. Povelje i prava na zaštitu ličnih podataka sadržanog u članu 8. Povelje.

U januaru 2017. godine Komisija je objavila Predlog uredbe o poštovanju privatnog života i zaštiti ličnih podataka u elektronskim komunikacijama, koja bi trebalo da zameni Direktivu o privatnosti i elektronskim komunikacijama. Reforma nastoji da uskladi odredbe kojima se uređuju elektronske komunikacije s novim sistemom

35 Direktiva 2002/58/EZ Evropskog parlamenta i Saveta od 12. jula 2002. o obradi ličnih podataka i zaštiti privatnosti u oblasti elektronskih komunikacija, SL L 201 (Direktiva o privatnosti i elektronskim komunikacijama).

36 Direktiva o privatnosti i elektronskim komunikacijama, član 4. stav 1.

37 *Ibid*., član 4. stav 2.

38 *Ibid*., član 4. stav 3.

zaštite podataka koji je uspostavljen Opštom uredbom o zaštiti podataka. Nova uredba će biti direktno primenjiva u celoj EU. Svi pojedinci će uživati isti nivo zaštite svojih elektronskih komunikacija, dok će telekomunikacioni operateri i kompanije ostvariti korist od jasnoće, pravne sigurnosti i postojanja jedinstvenog skupa pravila na području cele EU. Predloženi propisi o poverljivosti elektronskih komunikacija primenjivaće se i na nove učesnike na tržištu elektronskih komunikacionih usluga koje nisu obuhvaćene Direktivom o privatnosti i elektronskim komunikacijama. Direktivom su obuhvaćeni samo tradicionalni pružaoci telekomunikacionih usluga. Budući da dolazi do snažnog širenja upotrebe usluga kao što su Skype, WhatsApp, Facebook Messenger i Viber za slanje poruka ili pozivanje, te tzv. „over-the-top" (OTT) usluge sada će biti obuhvaćene oblašću primene uredbe i moraće da budu u skladu s njenim zahtevima u pogledu zaštite, privatnosti i bezbednosti podataka. U trenutku objave ovog priručnika, zakonodavni postupak donošenja propisa o e-privatnosti bio je još u toku.

Uredba br. 45/2001

Budući da je Direktiva o zaštiti podataka mogla da se primenjuje samo na države članice EU, bio je potreban dodatni pravni instrument kako bi se obezbedila zaštita podataka pri obradi ličnih podataka u institucijama i telima Evropske unije. To je učinjeno Uredbom (EZ) br. 45/2001 o zaštiti pojedinaca u vezi s obradom ličnih podataka u institucijama i telima Zajednice i o slobodnom kretanju takvih podataka (Uredba o zaštiti podataka u institucijama Evropske unije)[39].

Uredba br. 45/2001 sledi načela opšteg sistema zaštite podataka EU i njome se ta načela primenjuju na obradu podataka koju sprovode institucije i tela EU pri obavljanju svojih funkcija. Usto, njome se uspostavlja nezavisno nadzorno telo koje kontroliše primenu njenih odredbi, Evropski nadzornik za zaštitu podataka (ENZP). ENZP-u su dodeljene nadzorna ovlašćenja i dužnost nadzora nad obradom ličnih podataka u institucijama i telima EU, kao i primanje i istraživanje pritužbi za navodna kršenja propisa o zaštiti podataka. On takođe savetuje institucije i tela EU o svim pitanjima koja se odnose na zaštitu ličnih podataka, od predloga novog zakonodavstva do izrade nacrta internih pravila o obradi podataka.

U januaru 2017. godine Evropska komisija predstavila je predlog nove uredbe o obradi podataka u institucijama EU, kojom će se postojeća uredba staviti van snage.

39 Uredba (EZ) br. 45/2001 Evropskog parlamenta i Saveta od 18. decembra 2000. o zaštiti pojedinaca u vezi sa obradom ličnih podataka u institucijama i telima Zajednice i o slobodnom kretanju takvih podataka, SL 2001 L 8.

Kao i u slučaju reforme Direktive o privatnosti i elektronskim komunikacijama, reformom Uredbe br. 45/2001 modernizovaće se i uskladiti njene odredbe sa novim sistemom zaštite podataka koji je uspostavljen Opštom uredbom o zaštiti podataka.

Uloga Suda pravde Evropske unije (SPEU)

SPEU je nadležan za utvrđivanje da li je neka država članica ispunila svoje obaveze na osnovu zakonodavstva EU o zaštiti podataka, kao i za tumačenje zakonodavstva EU, kako bi se obezbedila njegova delotvorna i ujednačena primena u svim državama članicama. Od donošenja Direktive o zaštiti podataka 1995. godine nagomilala se znatna sudska praksa kojom se objašnjavaju oblast primene i značenje načelâ zaštite podataka i osnovnog prava na zaštitu ličnih podataka koji su garantovani članom 8. Povelje. Iako je Direktiva stavljena van snage, pa je sada na snazi novi pravni instrument, tj. Opšta uredba o zaštiti podataka, prethodna sudska praksa i dalje je relevantna i važeća za tumačenje i primenu načelâ EU o zaštiti podataka budući da su osnovna načela i koncepti Direktive o zaštiti podataka zadržani u GDPR-u.

1.2. Ograničenja prava na zaštitu ličnih podataka

Ključne tačke

- Pravo na zaštitu ličnih podataka nije apsolutno pravo. Ono se može ograničiti ako je potrebno zbog određenog cilja od opšteg interesa ili radi zaštite prava i sloboda drugih osoba.
- Uslovi za ograničenje prava na poštovanje privatnog života i zaštitu ličnih podataka navedeni su u članu 8. EKLJP-a i članu 52. stav 1. Povelje. Oni su razrađeni i protumačeni u okviru sudske prakse ESLJP-a i SPEU-a.
- Prema pravu zaštite podataka Saveta Evrope, obrada ličnih podataka predstavlja zakonito mešanje u pravo na poštovanje privatnog života i može se sprovoditi samo pod sledećim uslovima:
  - u skladu je sa zakonom
  - ima legitiman cilj
  - poštuje suštinu osnovnih prava i sloboda
  - nužna je i srazmerna u demokratskom društvu radi postizanja legitimne svrhe.

- Pravnim poretkom EU postavljaju se slični uslovi ograničenja ostvarivanja osnovnih prava zaštićenih Poveljom. Ograničenje bilo kojeg osnovnog prava, uključujući pravo na zaštitu ličnih podataka, može biti zakonito samo pod sledećim uslovima:
  - u skladu je sa zakonom
  - poštuje suštinu tog prava
  - shodno načelu srazmernosti, nužno je, i
  - ispunjava cilj od opšteg interesa koji priznaje EU ili potrebu za zaštitom prava drugih.

Osnovno pravo na zaštitu ličnih podataka na osnovu člana 8. Povelje nije apsolutno pravo, „već se mora razmatrati u vezi sa njegovom funkcijom u društvu"[40]. U članu 52. stav 1. Povelje tako se potvrđuje mogućnost nametanja ograničenja pri sprovođenju prava, poput onih iz članova 7. i 8. Povelje, pod uslovom da su takva ograničenja zakonita, da poštuju suštinu tih prava i sloboda i da su u skladu sa načelom srazmernosti nužna i da istinski ispunjavaju ciljeve od opšteg interesa koje je priznala EU ili pak potrebu zaštite tuđih prava i sloboda[41]. Slično tome, u sistemu EKLJP-a zaštita podataka garantovana je članom 8., a sprovođenje tog prava može biti ograničeno kada je to potrebno za ostvarenje legitimnog cilja. U ovom delu obuhvaćeni su uslovi za mešanje u pravo na osnovu EKLJP-a, kako se tumače u okviru sudske prakse ESLJP-a, kao i uslovi za zakonita ograničenja u skladu s članom 52. Povelje.

1.2.1. Zahtevi za opravdano mešanje iz Evropske konvencije o ljudskim pravima (EKLJP)

Obrada ličnih podataka može se smatrati mešanjem u pravo na poštovanje privatnog života ispitanika, koje je zaštićeno članom 8. EKLJP-a[42]. Kako je prethodno objašnjeno (vidi deo 1.1.1. i deo 1.1.4), za razliku od pravnog poretka EU, EKLJP-om se ne utvrđuje zaštita ličnih podataka kao posebno osnovno pravo. Zaštita ličnih podataka u sklopu Konvencije zapravo je deo prava zaštićenih u okviru prava na poštovanje privatnog života. Stoga ne bi svaka radnja koja uključuje obradu ličnih podataka bila

40 Videti, na primer, SPEU, spojeni predmeti C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen* [VV], 9. novembra 2010, stav 48.

41 *Ibid.*, stav 50.

42 ESLJP, *S. i Marper protiv Ujedinjenog Kraljevstva* [VV], br. 30562/04 i 30566/04, 8. decembra 2008, stav 67.

obuhvaćena oblašću primene člana 8. EKLJP-a. Da bi član 8. bio primenjen, prvo je potrebno utvrditi da li je narušen neki privatni interes ili privatni život osobe. ESLJP u svojoj sudskoj praksi pojam „privatnog života" smatra konceptom širokog značenja, koji obuhvata čak i neke aspekte profesionalnog života i ponašanja u javnosti. Takođe je presuđivao da je zaštita ličnih podataka važan deo prava na poštovanje privatnog života. Međutim, uprkos širokom tumačenju privatnog života, ne ugrožavaju sve vrste obrade podataka same po sebi prava zaštićena članom 8.

Kada ESLJP smatra da predmetni postupak obrade utiče na pravo pojedinca na poštovanje privatnog života, preispitaće da li je takvo mešanje u pravo opravdano. Pravo na poštovanje privatnog života nije apsolutno pravo, već se mora odmeriti i uskladiti sa drugim legitimnim interesima i pravima, bilo onima drugih osoba (privatnim interesima) ili onima društva u celini (javnim interesima).

Kumulativni uslovi u kojima mešanje može biti opravdano jesu sledeći.

U skladu sa zakonom

Prema sudskoj praksi Evropskog suda za ljudska prava, mešanje [u pravo na privatnost]je u skladu sa zakonom ako se zasniva na odredbi domaćeg zakonodavstva koje ima određene odlike. Zakon mora biti „dostupan dotičnim osobama i njegovi efekti moraju biti predvidivi"[43]. Pravilo je predvidivo „ako je formulisano dovoljno precizno da svaki pojedinac – uz, po potrebi, odgovarajuće savetovanje – može da reguliše svoje postupke"[44]. Zatim, „stepen preciznosti koji zakon mora imati u tom pogledu zavisi od konkretnog slučaja"[45].

43 ESLJP, *Amann protiv Švajcarske* [VV], br. 27798/95, 16. februara 2000, stav 50.; videti takođe ESLJP, *Kopp protiv Švajcarske*, br. 23224/94, 25. marta 1998, stav 55. i ESLJP, *Iordachi i drugi protiv Moldavije*, br. 25198/02, 10. februara 2009, stav 50.

44 ESLJP, *Amann protiv Švajcarske* [VV], br. 27798/95, 16. februara 2000., stav 56.; videti takođe ESLJP, *Malone protiv Ujedinjenog Kraljevstva*, br. 8691/79, 2. avgusta 1984, stav 66.; ESLJP, *Silver i dr. protiv Ujedinjenog Kraljevstva*, br. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. marta 1983, stav 88.

45 ESLJP, *Sunday Times protiv Ujedinjenog Kraljevstva*, br. 6538/74, 26. aprila 1979, stav 49.; videti takođe ESLJP, *Silver i dr. protiv Ujedinjenog Kraljevstva*, br. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. marta 1983, stav 88.

Primeri: U predmetu *Rotaru protiv Rumunije*[46] podnosilac predstavke je tvrdio da Obaveštajna služba Rumunije krši njegovo pravo na poštovanje privatnog života zbog toga što čuva i upotrebljava dosije s njegovim ličnim podacima. Evropski sud za ljudska prava utvrdio je da, iako je prema rumunskom zakonu dozvoljeno prikupljanje informacija koje utiču na nacionalnu bezbednost i njihovo beleženje i arhiviranje u tajnim spisima, granice za primenu tih ovlašćenja nisu propisane, već ih određuju nadležna tela. Na primer, domaćim zakonodavstvom nisu definisane vrste informacija koje smeju da se obrađuju, kategorije ljudi nad kojima smeju da se sprovode mere nadzora, okolnosti u kojima takve mere smeju da se sprovode niti postupak koji pri tome treba da se sledi. Zbog toga je ESLJP zaključio da domaće zakonodavstvo nije bilo u skladu sa zahtevom predvidivosti iz člana 8. Evropske konvencije o ljudskim pravima i da je taj član prekršen.

U predmetu *Taylor-Sabori protiv Ujedinjenog Kraljevstva*[47] podnosilac predstavke je bio podvrgnut nadzoru policije. Koristeći se „klonom" doušnika podnosiocaa predstavke policija je presretala poruke koje je primao. Tužilac je nakon toga uhapšen i optužen za zaveru u cilju nabavke kontrolisanih lekova. Tužilaštvo je optužbe protiv podnosioca predstavke delom zasnivalo na zapisima poruka od doušnika koji su nastali u isto vreme, a koje je policija transkribovala/prepisala. Međutim, u trenutku kad se podnosiocu predstavke sudilo, britanskim zakonodavstvom nije bilo regulisano presretanje komunikacije privatnim telekomunikacionim sistemima. Mešanje u njegova prava zato nije bilo „u skladu sa zakonom". ESLJP je zaključio da je time prekršen član 8. Konvencije.

Predmet *Vukota-Bojić protiv Švajcarske*[48] odnosio se na tajni nadzor podnositeljke predstavke, korisnice socijalnog osiguranja, koji su sprovodili privatni detektivi koje je angažovalo njeno osiguravajuće društvo. ESLJP je zaključio da, iako je predmetnu meru nadzora na koju se žalila podnositeljka prestvke naručilo privatno osiguravajuće društvo, tom društvu je država dala pravo da daje povlastice koje proizlaze iz obaveznog zdravstvenog osiguranja i da naplaćuje premije osiguranja. Država se ne može osloboditi odgovornosti na osnovu Konvencije tako što će preneti svoje obaveze na privatna tela ili

46 ESLJP, *Rotaru protiv Rumunije* [VV], br. 28341/95, 4. maja 2000., stav 57.; videti takođe ESLJP, *Udruženje za evropsku integraciju i ljudska prava i Ekimdzhiev protiv Bugarske*, br. 62540/00, 28. juna 2007.; ESLJP, *Shimovolos protiv Rusije*, br. 30194/09, 21. juna 2011. i ESLJP, *Vetter protiv Francuske*, br. 59842/00, 31. maja 2005.

47 ESJLP, *Taylor-Sabori protiv Ujedinjenog Kraljevstva*, br. 47114/99, 22. oktobra 2002.

48 ESLJP, *Vukota-Bojić protiv Švajcarske*, br. 61838/10, 18. oktobra 2016., stav 77.

pojedince. Da bi mešanje u prava iz člana 8. EKLJP-a bilo „u skladu sa zakonom", domaćim zakonodavstvom morale su biti propisane odgovarajuće mere zaštite od zloupotrebe. U navedenom predmetu ESLJP je zaključio da je došlo do povrede člana 8. Konvencije budući da u domaćem zakonodavstvu nije bila dovoljno jasno navedena oblast primene i način sprovođenja ovlašćenja za vršenje tajnog nadzora osigurane osobe, koja su dodeljena osiguravajućim društvima koja deluju kao organ javne vlasti u sporovima u vezi sa osiguranjem. Tačnije, zakonodavstvo nije sadržalo dovoljne mere zaštite od zloupotrebe.

Legitimna svrha/cilj

Legitimna svrha može da se odnosi ili na jedan od navedenih javnih interesa ili na zaštitu prava i sloboda drugih. U skladu s članom 8. stav 2. EKLJP-a, legitimni ciljevi koji bi mogli da opravdaju mešanje u prava pojedinca jesu interesi nacionalne bezbednosti, javni red i mir ili ekonomska dobrobit zemlje, sprečavanje nereda ili zločina, zaštita zdravlja ili morala kao i zaštita prava i sloboda drugih.

Primer: U predmetu *Peck protiv Ujedinjenog Kraljevstva*[49] podnosilac predstavke je pokušao da izvrši samoubistvo na ulici tako što je sam sebi presekao vene, a nije bio svestan da ga snima kamera video-nadzora/zatvorenog kola (CCTV). Policija je gledala snimke kamera zatvorenog kola i spasila ga, nakon čega je snimke prosledila medijima, koji su ih objavili bez zamagljivanja lica podnosioca predstavke. ESLJP je zaključio da nije bilo relevantnih niti dovoljnih razloga kojima bi se opravdalo direktno otkrivanje/obelodanjivanje snimaka javnosti bez pristanka podnosioca predstavke ili prikrivanja njegovog identiteta. ESLJP je stoga zaključio da je došlo do povrede člana 8. Konvencije.

Neophodno u demokratskom društvu

ESLJP je istakao da „pojam nužnosti podrazumeva da je mešanje odgovor na nužnu društvenu potrebu i naročito da je srazmerno legitimnom cilju koja nastoji da postigne"[50]. Prilikom ocenjivanja da li je neka mera neophodna da bi se ispunila nužna društvena potreba, ESLJP preispituje njenu relevantnost i primerenost s obzirom na cilj koji treba da se ostvari. U tu svrhu može da se razmotri da li se mešanjem pokušava rešavanje

49 ESLJP, *Peck protiv Ujedinjenog Kraljevstva*, br. 44647/98, 28. januara 2003, stav 85.

50 ESLJP, *Leander protiv Švedske*, br. 9248/81, 26. marta 1987, stav 58.

problema koji bi inače imao štetan efekat na društvo, da li postoje dokazi da se mešanjem može ublažiti takav štetan efekat i koji su širi društveni stavovi o tom pitanju[51]. Na primer, prikupljanjem i čuvanjem ličnih podataka određenih pojedinaca za koje se pokaže da imaju veze sa terorističkim pokretima bezbednosne službe bi se mešale u pravo pojedinaca na poštovanje privatnog života, ali takve radnje ujedno služe i ozbiljnoj, nužnoj društvenoj potrebi: nacionalnoj bezbednosti i borbi protiv terorizma. Da bi kriterijum „nužnosti" bio ispunjen, mešanje takođe mora biti srazmerno. U sudskoj praksi ESLJP-a srazmernost je obuhvaćena konceptom nužnosti. Da bi mešanje u prava zaštićena EKLJP-om bilo srazmerno, ono ne sme da izlazi van okvira onoga što je nužno za ispunjenje legitimne svrhe koja treba da se ostvari. Važni činioci koje treba uzeti u obzir prilikom utvrđivanja srazmernosti jesu opseg mešanja, prvenstveno broj osoba koje će time biti pogođene, zaštitne mere ili upozorenja uspostavljena kako bi se ograničio njegov opseg ili štetni efekti na prava pojedinaca[52].

Primer: U predmetu *Khelili protiv Švajcarske*[53] policija je vršeći proveru utvrdila da podnositeljka predstavke poseduje posetnice na kojima je pisalo: „Simpatična, zgodna žena u kasnim tridesetima želi da upozna muškarca da se povremeno sastanu uz piće ili zajedno izađu. Telefonski br. [...]." Podnositeljka predstavke se žalila da ju je policija nakon pronalaska posetnice u svojoj evidenciji zapisala kao prostitutku, iako je ona uporno tvrdila da se time ne bavi. Podnositeljka predstavke je zatražila brisanje reči „prostitutka" iz računara evidencije policije. ESLJP je utvrdio da, u načelu, zadržavanje ličnih podataka pojedinca, zbog mogućnosti da ta osoba učini drugo krivično delo, u određenim okolnostima može da bude srazmerno. Međutim, u slučaju podnositeljke predstavke tvrdnja o navodnoj nezakonitoj prostituciji činila se previše nejasnom i uopštenom i nije bila potkrepljena konkretnim činjenicama, jer ona nikada nije bila osuđena za nezakonitu prostituciju, pa uslov „nužne društvene potrebe" u smislu člana 8. Konvencije nije bio ispunjen. Smatrajući da su nadležna tela odgovorna za dokazivanje tačnosti pohranjenih podataka o podnositeljki predstavke i uzimajući u obzir ozbiljnost mešanja u njena prava, ESLJP je presudio da dugotrajno zadržavanje reči „prostitutka" u policijskoj evidenciji nije bilo nužno u demokratskom društvu. ESLJP je stoga zaključio da je došlo do povrede člana 8. Konvencije.

51 Radna grupa za zaštitu podataka iz člana 29. (Radna grupa iz člana 29.) (2014.), Opinion on the application of the necessity and proportionality concepts and data protection within the law enforcement sector, WP 211, Bruxelles, 27. februara 2014, str. 7–8.

52 *Ibid*., str. 9–11.

53 ESLJP, *Khelili protiv Švajcarske*, br. 16188/07, 18. oktobra 2011.

Primer: U predmetu *S. i Marper protiv Ujedinjenog Kraljevstva*[54] oba podnosioca predstavki su uhapšena i optužena za krivična dela. Policija je uzela njihove otiske prstiju i uzorke DNK, kako je propisano Zakonom o policiji i dokazima u krivičnom postupku Ujedinjenog Kraljevstva (engl. *Police and Criminal Evidence Act*). Podnosioci predstavki nikada nisu osuđeni za krivična dela: jedan od njih je oslobođen na sudu, a krivični postupak protiv drugog je obustavljen. Uprkos tome, policija je zadržala i sačuvala njihove otiske prstiju, DNK profile i uzorke ćelija u bazi podataka, a domaćim zakonodavstvom dozvoljeno je njihovo zadržavanje bez vremenskog ograničenja. Ujedinjeno Kraljevstvo je tvrdilo da je zadržavanje materijala pomoglo u otkrivanju budućih učinilaca krivičnih dela, pa je tako nastojala da ostvari legitimni cilj prevencije i otkrivanja zločina, ali ESLJP je to smatrao neopravdanim mešanjem u pravo podnosilaca predstavki na poštovanje privatnog života. ESLJP je istakao da prema osnovnim načelima zaštite podataka zadržavanje ličnih podataka mora da bude srazmerno s obzirom na svrhu prikupljanja i da periodi zadržavanja moraju biti ograničena. ESLJP je prihvatio argument da je proširivanje baze podataka na DNK profile i osuđenih osoba i svih pojedinaca koji su osumnjičeni, ali ne i osuđeni, moglo da doprinese otkrivanju i prevenciji krivičnih dela u Ujedinjenom Kraljevstvu. Međutim, bio je „iznenađen sveobuhvatnim i neselektivnim karakterom ovlašćenja na zadržavanje podataka"[55].

S obzirom na brojne genetske i zdravstvene informacije sadržane u uzorcima ćelija, mešanje u pravo podnosilaca predstavki na privatni život bilo je posebno ozbiljno. Otisci prstiju i uzorci mogli su da se uzimaju od uhapšenih i neograničeno zadržavaju u policijskoj bazi podataka, nezavisno od prirode i težine učinjenog dela, čak i za manje prekršaje za koje nije predviđena zatvorska kazna. Osim toga, mogućnost da se podaci o oslobođenim pojedincima izbrišu iz baze podataka bila je ograničena. Na kraju, ESLJP je posebno uzeo u obzir činjenicu da je jedan od podnosilaca predstavki u trenutku hapšenja imao jedanaest godina. Zadržavanje ličnih podataka maloletnika koji nije osuđen može biti posebno štetno zbog njegove osetljivosti i važnosti njegovog razvoja i integracije u društvo[56]. Sud je doneo jednoglasnu odluku da je zadržavanje podataka predstavljalo nesrazmerno mešanje u pravo na privatni život koje ne može da se smatra nužnim u demokratskom društvu.

54 ESLJP, *S. i Marper protiv Ujedinjenog Kraljevstva* [VV], br. 30562/04 i 30566/04, 4. decembra 2008.

55 *Ibid.*, stav 119.

56 *Ibid.*, stav 124.

Primer: U predmetu *Leander protiv Švedske*[57] ESLJP je presudio da tajna provera osoba koje se prijavljuju za zaposlenje na radnim mestima važnim za nacionalnu bezbednost nije sama po sebi u suprotnosti sa zahtevom nužnosti u demokratskom društvu. Posebne zaštitne mere propisane domaćim zakonodavstvom za zaštitu interesa ispitanika – na primer, kontrole koje sprovodi parlament i kancelar za pravosuđe – dovele su do zaključka ESLJP-a da je švedski sistem za kontrolu osoblja ispunio zahteve iz člana 8. stav 2. EKLJP-a. Imajući na umu da je imala na raspolaganju široko polje slobodne procene, tužena država je s pravom smatrala da su u slučaju podnosioca predstavke interesi nacionalne bezbednosti bili važniji od pojedinačnih. ESLJP je zato zaključio da nije došlo do povrede člana 8. Konvencije.

1.2.2. Uslovi za zakonita ograničenja u skladu sa Poveljom Evropske unije o osnovnim pravima

Struktura i tekst Povelje razlikuju se od strukture i teksta Evropske konvencije o ljudskim pravima. U Povelji se ne javlja koncept mešanja u garantovana prava, ali u njoj je sadržana odredba o ograničenju/ima pri ostvarivanju prava i sloboda priznatih Poveljom.

Prema članu 52. stav 1., ograničenja pri ostvarivanju prava i sloboda priznatih Poveljom i, u skladu s tim, ostvarivanju prava na zaštitu ličnih podataka, prihvatljiva su samo pod sledećim uslovima:

- da su propisana zakonom,
- da poštuju suštinu prava na zaštitu podataka,
- da su nužna, shodno načelu srazmernosti[58] i
- da ispunjavaju ciljeve od opšteg interesa koje priznaje Unija ili potrebu za zaštitom prava i sloboda drugih.

57 ESLJP, *Leander protiv Švedske*, br. 9248/81, 26. marta 1987, st. 59 i 67.

58 Za procenu nužnosti mera kojima se ograničava osnovno pravo na zaštitu ličnih podataka videti : EDPS (2017.), *Necessity Toolkit* (Paket alata za određivanje nužnosti mera), Bruxelles, 11. aprila 2017.

Budući da je zaštita ličnih podataka zasebno i samostalno osnovno pravo u pravnom poretku EU, zaštićeno članom 8. Povelje, svaka obrada ličnih podataka sama po sebi čini mešanje u to pravo. Nevažno je da li su ti lični podaci u vezi sa privatnim životom pojedinca, da li su osetljivi i da li je ispitanicima na bilo koji način prouzrokovana neprijatnost. Da bi bilo zakonito, mešanje mora da ispunjava sve uslove navedene u članu 52. stav 1. Povelje.

Propisano zakonom

Ograničenja prava na zaštitu ličnih podataka moraju biti propisana zakonom. Ovim uslovom se podrazumeva da ograničenja moraju da se zasnivaju na pravnoj osnovi koja je dovoljno pristupačna i predvidiva i dovoljno precizno formulisana kako bi pojedincima omogućila da razumeju svoje obaveze i kontrolišu svoje postupke. Pravna osnova takođe mora da pruža jasnu definiciju oblasti primene i načina izvršavanja ovlašćenja nadležnih tela kako bi se pojedinci zaštitili od proizvoljnog mešanja. Takvo tumačenje slično je zahtevu za „zakonitim mešanjem" iz sudske prakse ESLJP-a[59], a smatra se i da značenje izraza „propisano zakonom", koji se upotrebljava u Povelji, treba da bude isto sa značenjem koje on ima u kontekstu EKLJP-a[60]. Sudska praksa ESLJP-a, a posebno koncept „kvaliteta zakona" koji je razvio tokom godina, važna je stavka koju SPEU mora da uzme u obzir prilikom tumačenja oblasti primene člana 52. stav 1. Povelje[61].

Poštovanje suštine prava

U pravnom poretku EU svako ograničenje osnovnih prava zaštićenih Poveljom mora poštovati suštinu tih prava. To znači da se ne mogu opravdati ograničenja koja su toliko opsežna i ozbiljna da zbog njih neko osnovno pravo gubi svoj osnovni smisao. Ako je suština prava ugrožena, ograničenje se mora smatrati nezakonitim i nije potrebna dalja procena da li ono služi cilju od opšteg interesa i da li zadovoljava kriterijume nužnosti i srazmernosti.

59 EDPS (2017.), *Paket alata za određivanje nužnosti mera*, Bruxelles, 11. aprila 2017., str. 4.; videti i SPEU, *Mišljenje 1/15 Suda (veliko Veće)*, 26. jula 2017.

60 SPEU, spojeni predmeti C-203/15 i C-698/15, *Tele2 Sverige AB protiv Post- och telestyrelsen* i *Secretary of State for the Home Department protiv Toma Watsona, Petera Bricea, Geoffreyja Lewisa*, Mišljenje nezavisnog advokata Henrika Saugmandsgaarda Øea od 19. jula 2016, stav 140.

61 SPEU, C-70/10, *Scarlet Extended SA protiv Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, Mišljenje nezavisnog advokata Pedra Cruza Villalóna od 14. aprila 2011, stav 100.

Primer: Predmet *Schrems*[62] odnosio se na zaštitu pojedinaca u pogledu prenosa njihovih ličnih podataka u treće zemlje, u ovom slučaju u Sjedinjene Američke Države. Gospodin Šrems (nem. Schrems), austrijski državljanin i dugogodišnji korisnik društvene mreže Fejsbuk, podneo je prigovor irskom nadležnom telu za zaštitu podataka kako bi se žalio na prenos njegovih ličnih podataka iz irske podružnice kompanije Fejsbuk u sedište kompanije Fejsbuk u SAD. kao i na servere u SAD, gde su podaci obrađivani. Tvrdio je da zakoni i praksa u SAD ne pružaju dovoljnu zaštitu ličnih podataka koji se prenose na državno područje SAD kada se uzmu u obzir informacije koje je 2013. američki uzbunjivač Edvard Snouden razotkrio u vezi s aktivnostima nadzora američkih obaveštajnih službi. Snouden je objavio da je američka Nacionalna bezbednosna agencija (engl. National Security Agency) imala direktan pristup računarskim serverima društvenih mreža kao što je Fejsbuk i da je mogla da čita sadržaj razgovora i privatnih poruka.

Prenosi podataka u SAD zasnivali su se na odluci Komisije o primerenosti, donesenoj 2000. godine, kojom su omogućeni prenosi društvenim mrežama u SAD koje su same potvrdile da će štititi lične podatke prenesene iz EU i pridržavati se tzv. principa „sigurne luke". Kada je predmet iznesen pred SPEU, on je preispitao valjanost odluke Komisije u kontekstu Povelje. SPEU je podsetio da zaštita osnovnih prava u EU zahteva da se izuzeća i ograničenja tih prava primenjuju samo ako su strogo nužna. SPEU je smatrao da propis koji omogućava javnim telima neograničen pristup sadržaju elektronskih komunikacija „ugrožava suštinu osnovnog prava na poštovanje privatnog života koje je garantovano u članu 7. Povelje". Pravo bi izgubilo smisao ako bi javne vlasti SAD bila ovlašćene na bezrazložno pristupanje komunikacijama, bez objektivnog opravdanja koje se temelji na konkretnim razlozima nacionalne bezbednosti ili prevencije krivičnih dela koja se povezuju sa konkretnim pojedincem i bez obezbeđivanja odgovarajućih zaštitnih mera od zloupotrebe ovlašćenja za te nadzorne prakse.

Usto, SPEU je istakao da „propis koji pojedincima ne pruža nikakvu mogućnost korišćenja pravnih sredstava radi pristupa ličnim podacima koji se na njih odnose, ili radi ispravke ili brisanja takvih podataka," nije u skladu s osnovnim pravom na delotvornu sudsku zaštitu (član 47. Povelje). Stoga Odlukom o sigurnoj luci nije obezbeđen nivo zaštite osnovnih prava u SAD koji bi u osnovi

62 SPEU, C-362/14, *Maximillian Schrems protiv Data Protection Commissioner* [VV], 6. oktobra 2015.

bio iste vrednosti kao onaj koji je zagarantovan unutar EU na osnovu direktive tumačene u kontekstu Povelje. SPEU je zato poništio Odluku[63].

Primer: U predmetu *Digital Rights Ireland*[64] SPEU je ispitao usklađenost Direktive 2006/24/EZ (Direktiva o zadržavanju podataka) sa članovima 7. i 8. Povelje. Direktiva je nalagala pružaocima elektronskih komunikacionih usluga obavezu zadržavanja podataka o potrošnji i lokaciji najmanje šest meseci, do najviše 24 meseca, kao i omogućivanja pristupa nadležnih nacionalnih tela tim podacima radi sprečavanja, istrage, otkrivanja i gonjenja teških krivičnih dela. Direktivom nije dozvoljeno zadržavanje sadržaja elektronskih komunikacija. SPEU je istakao da podaci koje pružaoci usluga moraju da zadržavaju u skladu sa Direktivom uključuju podatke potrebne za pronalaženje i identifikaciju izvora i odredišta komunikacije, datuma, vremena i trajanja komunikacije, telefonskih brojeva sa kojih se poziva i koji se pozivaju kao i IP adresa. Ti podaci, „uzeti zajedno, mogu omogućiti donošenje vrlo preciznih zaključaka o privatnom životu osoba čiji su podaci zadržani, kao što su svakodnevne navike, mesta trajnih ili privremenih boravišta, dnevna ili druga kretanja, obavljane aktivnosti, društveni odnosi i društvene sredine koje su te osobe posećivale".

Stoga zadržavanje ličnih podataka na osnovu Direktive čini posebno ozbiljno mešanje u prava na privatnost i zaštitu ličnih podataka. Međutim, SPEU je smatrao da mešanje nije negativno uticalo na suštinu tih prava. Kad je reč o pravu na privatnost, njegova suština nije bila ugrožena jer Direktivom nije bilo dozvoljeno sticanje saznanja o samom sadržaju elektronskih komunikacija. Slično tome, suština prava na zaštitu ličnih podataka nije bila ugrožena jer se Direktivom od pružaoca elektronskih komunikacionih usluga zahtevalo da poštuju određene principe zaštite podataka i bezbednosti podataka, kao i da u tu svrhu sprovedu odgovarajuće tehničke i organizacione mere.

63 Odluka SPEU da Odluku Komisije 520/2000/EZ proglasi nevažećom takođe se temeljila na drugim osnovama koje se razmatraju u drugim delovima priručnika. SPEU je prvenstveno smatrao da se Odlukom nezakonito ograničavaju ovlašćenja domaćih nadzornih tela za zaštitu podataka. Usto, u sistemu koji se zasniva na načelu „sigurne luke" pojedincima nisu bili dostupni nikakvi pravni lekovi ako su hteli da pristupe ličnim podacima o sebi i/ili obezbede njihovo ispravljanje ili brisanje. Stoga je ugrožena i suština osnovnog prava na delotvornu sudsku zaštitu, garantovanog članom 47. Povelje.

64 SPEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr.* i *Kärntner Landesregierung i dr.* [VV], 8. aprila 2014.

Nužnost i srazmernost

Članom 52. stav 1. Povelje propisuje se da su, shodno načelu srazmernosti, , ograničenja ostvarivanja osnovnih prava i sloboda priznatih Poveljom moguća samo ako su nužna.

Ograničenje može biti **nužno** ako je potrebno doneti mere za ostvarenje cilja od javnog interesa, ali nužnost, kako je tumači SPEU, takođe podrazumeva da donesene mere moraju da budu manje nametljive u odnosu na druge mogućnosti ostvarivanja istog cilja. Za ograničenja prava na poštovanje privatnog života i zaštitu ličnih podataka SPEU primenjuje strogi „test nužnosti", smatrajući da se „izuzeća i ograničenja moraju primenjivati samo ako su strogo nužna". Ako se neko ograničenje smatra strogo nužnim, treba oceniti i da li je srazmerno.

Srazmernost znači da prednosti koje proizlaze iz ograničenja treba da prevagnu nad nedostacima koje ograničenje izaziva za ostvarivanje predmetnih osnovnih prava[65]. Kako bi se umanjili nedostaci i rizici za ostvarivanje prava na privatnost i zaštitu podataka, važno je da ograničenja sadrže odgovarajuće zaštitne mere.

Primer: U predmetu *Volker und Markus Schecke*[66] SPEU je zaključio da su nametanjem obaveze objavljivanja ličnih podataka svih fizičkih lica koja su bila korisnici novčane pomoći iz određenih poljoprivrednih fondova bez pravljenja razlike na osnovu bitnih kriterijuma kao što su periodi tokom kojih su te osobe primale novčanu pomoć, učestalost ili prirodu i iznos pomoći, Savet i Komisija prekoračili ograničenja propisana načelom srazmernosti.

Stoga je SPEU zaključio da je određene odredbe Uredbe Saveta (EZ) br. 1290/2005 nužno proglasiti nevažećim, a Uredbu br. 259/2008 proglasiti nevažećom u celosti[67].

65 EDPS (2017.), *Necessity Toolkit* (Paket alata za određivanje nužnosti mera), str. 5.

66 SPEU, spojeni predmeti C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen* [VV], 9. novembra 2010, st. 89 i 86.

67 Uredba Saveta (EZ) br. 1290/2005 od 21. juna 2005. o finansiranju zajedničke poljoprivredne politike, SL 2005 L 209; Uredba Komisije (EZ) br. 259/2008 od 18. marta 2008. o utvrđivanju detaljnih pravila za primenu Uredbe Saveta (EZ) br. 1290/2005 u pogledu objavljivanja informacija o korisnicima sredstava iz Evropskog fonda za garancije u poljoprivredi (EFJP) i Evropskog poljoprivrednog fonda za ruralni razvoj (EPFRR), SL 2008 L 76.

Primer: U predmetu *Digital Rights Ireland*[68] SPEU je zaključio da mešanjem u pravo na privatnost koje je izazvano primenom Direktive o zadržavanju podataka nije ugrožena suština tog prava, jer se Direktivom zabranjuje zadržavanje sadržaja elektronskih komunikacija. Međutim, zaključio je i da Direktiva nije usklađena sa članovima 7. i 8. Povelje, pa ju je proglasio nevažećom. Budući da se podaci o potrošnji i lokaciji, grupni i razmatrani kao celina, mogu analizirati i pružaju detaljnu sliku privatnog života pojedinaca, to čini ozbiljno mešanje u ta prava. SPEU je uzeo u obzir činjenicu da se Direktivom zahteva zadržavanje svih metapodataka o fiksnoj i mobilnoj telefoniji, pristupu internetu, internet elektronskoj pošti i internet telefoniji, koji se primenjuju na sva sredstva elektronske komunikacije, čija je upotreba vrlo raširena u svakodnevnom životu. To je zapravo predstavljalo mešanje koje je uticalo na celokupnu populaciju Evrope. Kada se u obzir uzmu opseg i ozbiljnost takvog mešanja, prema mišljenju SPEU zadržavanje podataka o prometu i lokaciji može se opravdati samo svrhom borbe protiv teških krivičnih dela. Usto, Direktivom nisu utvrđeni nikakvi objektivni kriterijumi kojima bi se obezbedilo da pristup nadležnih nacionalnih tela zadržanim podacima bude ograničen na ono što je strogo nužno. Direktiva takođe ne sadrži materijalne i procesne uslove kojima se uređuju pristup domaćih organa vlasti zadržanim podacima koji nisu podvrgnuti prethodnom preispitivanju suda ili drugog nezavisnog tela i njihova upotreba.

SPEU je do sličnog zaključka došao i u spojenim predmetima *Tele2 Sverige AB protiv Post- och telestyrelsen* i *Secretary of State for the Home Department protiv Toma Watsona i drugih*[69]. Ti predmeti su se odnosili na zadržavanje podataka o potrošnji i lokaciji koji obuhvataju „sve pretplatnike i registrovane korisnike kao i [...] sva sredstva elektronske komunikacije" i metapodatke, pri čemu se ne predviđa „razlikovanje, ograničenje ili izuzetak s obzirom na cilj koji treba da se postigne"[70]. U ovom predmetu uslov zadržavanja podataka o pojedincu nije bio da li je on ili nije direktno ili indirektno povezan sa teškim krivičnim delima, niti da li je njegova komunikacija bila važna za nacionalnu bezbednost. S obzirom na nedostatak nužne veze između zadržanih podataka i pretnje javnoj bezbednosti ili ograničenja vremenskog perioda ili geografskog

68 SPEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr. i Kärntner Landesregierung i dr.* [VV], 8. aprila 2014, stav 39.

69 SPEU, spojeni predmeti C-203/15 i C-698/15, *Tele2 Sverige AB protiv Post- och telestyrelsen i Secretary of State for the Home Department protiv Toma Watsona i drugih* [VV], 21. decembra 2016, st. 105 i 106.

70 *Ibid.*, stav 105.

područja, SPEU je zaključio da domaće zakonodavstvo prelazi granice onoga što je strogo nužno za svrhu borbe protiv teških krivičnih dela[71].

Sličan pristup u pogledu nužnosti je primenio i Evropski nadzornik za zaštitu podataka u svom *Paketu alata za određivanje nužnosti mera*[72]. Paket alata služi za procenu usklađenosti predloženih mera sa pravom EU o zaštiti podataka. Paket je razvijen kako bi pomogao donosiocima politika i zakonodavcima u EU koji su zaduženi za pripremu ili preispitivanje mera koje uključuju obradu ličnih podataka i kojima se ograničava pravo na zaštitu ličnih podataka, kao i druga prava i slobode utvrđene u Povelji.

Ciljevi od opšteg interesa

Da bi bilo opravdano, svako ograničenje ostvarivanja prava priznatih Poveljom mora u suštini da ispunjava ciljeve opšteg interesa koje priznaje Unija ili potrebu za zaštitom prava i sloboda drugih. Kad je reč o potrebi zaštite prava i sloboda drugih, pravo na zaštitu ličnih podataka često je povezano sa drugim osnovnim pravima. U delu 1.3. prikazana je detaljna analiza tih odnosa. Ciljevi od opšteg interesa uključuju opšte ciljeve EU utvrđene u članu 3. Ugovora o Evropskoj uniji (UEU), kao što su unapređenje mira i dobrobiti njenih nacija, socijalne pravde i zaštite, uspostavljanje oblasti slobode, bezbednosti i pravde na kojoj je obezbeđeno slobodno kretanje osoba zajedno sa odgovarajućim merama u pogledu sprečavanja i suzbijanja kriminala i drugih ciljeva i interesa zaštićenih pojedinim odredbama ugovora[73]. U tom pogledu se u Opštoj uredbi o zaštiti podataka dodatno razrađuje član 52. stav 1. Povelje: u članu 23. stav 1. Uredbe navodi se niz ciljeva od opšteg interesa koji se smatraju legitimnim za ograničavanje prava pojedinaca, pod uslovom da se takvim ograničenjem poštuje suština prava na zaštitu ličnih podataka i da je ono nužno i srazmerno. Među navedenim ciljevima od javnog interesa su nacionalna bezbednost i odbrana, sprečavanje krivičnih dela, zaštita važnih ekonomskih i finansijskih interesa EU ili država članica, javno zdravstvo i socijalna bezbednost.

Važno je dovoljno detaljno definisati i objasniti cilj od opšteg interesa koji nastoji da se ostvari ograničenjem, jer će se nužnost ograničenja proceniti s obzirom na taj element. Jasan i detaljan opis cilja ograničenja i predloženih mera neophodan

71 *Ibid.*, stav 107.

72 EDPS (2017.), *Paket alata za određivanje nužnosti mera*, Bruxelles, 11. aprila 2017.

73 Objašnjenja koja se odnose na Povelju Evropske unije o osnovnim pravima (2007/C 303/02), SL 2007 br. C 303, str. 17.–35.

je za omogućavanje procene njegove nužnosti[74]. Cilj koji nastoji da se ostvari, kao i nužnost i srazmernost ograničenja, usko su povezani.

Primer: Predmet *Schwarz protiv Stadt Bochum*[75] odnosio se na ograničenje prava na poštovanje privatnog života i prava na zaštitu ličnih podataka koje proizlazi iz uzimanja i čuvanja otisaka prstiju kada države članice izdaju pasoša[76]. Tužilac je podneo zahtev za izradu pasoša u gradu Bohumu u Nemačkoj, ali odbio je da da otiske prstiju. Posle toga, grad Bohum odbio je njegov zahtev za izradu pasoša. On je zatim pokrenuo postupak pred nemačkim sudom radi izdavanja pasoša bez davanja otisaka prstiju. Nemački sud je uputio prethodno pitanje SPEU, uz pitanje da li član 1. stav 2. Uredbe br. 2252/2004 o standardima za bezbednosna obeležja i biometrijske podatke u pasošima i putnim ispravama, koje izdaju države članice, može da se smatra valjanim.

SPEU je istakao da otisci prstiju **predstavljaju lične podatke,** jer objektivno sadrže jedinstvene informacije o pojedincima koje omogućavaju njihovu preciznu identifikaciju, a uzimanje i čuvanje otisaka prstiju predstavljaju obradu. Takva obrada, uređena članom 1 stav 2. Uredbe br. 2252/2004, predstavlja pretnju pravima na poštovanje privatnog života i zaštitu ličnih podataka[77]. Međutim, član 52. stav 1. Povelje omogućava postavljanje ograničenja pri ostvarivanju tih prava, pod uslovom da su takva ograničenja zakonita, da poštuju suštinu tih prava, da su u skladu sa načelom srazmernosti nužna i da istinski ispunjavaju ciljeve od opšteg interesa koje je priznala Unija, ili potrebu zaštite prava i sloboda drugih.

U ovom predmetu SPEU je prvo istakao da se ograničenje koje proizlazi iz uzimanja i čuvanja otisaka prstiju prilikom izdavanja pasoša mora smatrati **zakonitim** budući da su takvi postupci propisani članom 1. stav 2. Uredbe br. 2252/2004. Drugo, navedena Uredba osmišljena je kako bi se sprečilo falsifikovanje pasoša i njihova zloupotreba. Stoga član 1. stav 2. između ostalog služi za sprečavanje nezakonitog ulaska u EU, čime se nastoji da se ispuni cilj od opšteg interesa koji priznaje Unija. Treće, na osnovu dokaza koji su bili dostupni SPEU-u nije bilo jasno, niti se tvrdilo, da se ograničenjima za ostvarivanje tih prava u ovom

74 EDPS (2017.), *Necessity Toolkit* (Paket alata za određivanje nužnosti mera), Bruxelles, 11. aprila 2017, str. 4.

75 SPEU, C-291/12, *Michael Schwarz protiv Stadt Bochum*, 17. oktobra 2013.

76 *Ibid*., st. od 33 do 36.

77 *Ibid*., st. od 27 do 30.

predmetu nije poštovala suština tih prava. Četvrto, za čuvanje otisaka prstiju na vrlo sigurnom mediju za čuvanje, koje predviđa taodredba,potrebna je sofisticirana tehnologija. Takvim čuvanjem će se verovatno smanjiti opasnost od falsifikovanja pasoša i olakšati rad tela nadležnih za proveru autentičnosti pasoša na granicama EU. Činjenica da ta metoda nije potpuno pouzdana nije odlučujuća. Iako se ovom metodom ne sprečava prijem svih neovlašćenih osoba, dovoljna je da se znatno smanji verovatnoća njihovog prijema. S obzirom na navedeno, SPEU je zaključio da je uzimanje i čuvanje otisaka prstiju utvrđeno u članu 1. stav 2. Uredbe br. 2252/2004 bilo primereno za ostvarenje ciljeva te Uredbe, a time i cilja sprečavanja nezakonitog ulaska u EU[78].

SPEU je zatim ocenio da li je takva obrada **nužna**, primećujući da je predmetni postupak uključivao uzimanje otisaka samo dva prsta, koji su, štaviše, uglavnom vidljivi drugima, pa zato nije reč o postupku intimne prirode. Njime se takođe ne izaziva nikakva posebna fizička ili mentalna neprijatnost osobi čiji se otisci uzimaju, svakako ništa veća nego snimanje fotografije lica te osobe. Takođe treba napomenuti da je jedina stvarna alternativa uzimanju otisaka prstiju u ovom postupku pred SPEU bilo skeniranje zenica oka. Ništa u spisu predmeta podnesenom SPEU-u nije upućivalo na to da bi se potonjim postupkom manje mešalo u prava priznata članovima 7. i 8. Povelje nego uzimanjem otisaka prstiju. Dalje, u pogledu delotvornosti tih dveju metoda, poznato je da tehnologija prepoznavanja zenica još nije dovoljno napredna kao tehnologija prepoznavanja otisaka prstiju i trenutno je znatno skuplja od postupka za upoređivanje otisaka prstiju, tako da je zbog toga manje prikladna za opštu primenu. Prema tome, SPEU nije bio ubeđen ni u kakve mere koje bi istovremeno bile dovoljno delotvorne u ostvarenju cilja zaštite od zloupotrebe pasoša i predstavljale manju pretnju pravima priznatim članovima 7. i 8. Povelje od mera koje proizlaze iz metode upotrebe otisaka prstiju[79].

SPEU je napomenuo da se u članu 4. stav 3. Uredbe br. 2252/2004 izričito navodi da se otisci prstiju mogu upotrebiti samo za proveru autentičnosti pasoša i identiteta njegovog vlasnika, a u članu 1. stav 2. Uredbe nije utvrđeno čuvanje otisaka prstiju, osim unutar samog pasoša, koji pripada isključivo vlasniku. Stoga, Uredba ne pruža pravnu osnovu za centralizovano čuvanje podataka prikupljenih na osnovu nje, niti za upotrebu takvih podataka u druge svrhe osim

78 *Ibid*., st. od 35 do 45.

79 SPEU, C-291/12, *Michael Schwarz protiv Stadt Bochum*, 17. oktobra 2013, st. od 46 do 53.

sprečavanja nezakonitog ulaska u EU[80]. S obzirom na sve navedeno, SPEU je zaključio da razmatranjem pitanja koje mu je upućeno nije otkriveno ništa što bi moglo da utiče na valjanost člana 1. stav 2. Uredbe br. 2252/2004.

Odnos između Povelje i Evropske konvencije o ljudskim pravima (EKLJP)

Uprkos različitom načinu izražavanja, uslovi za zakonita ograničenja prava iz člana 52 stav 1. Povelje podsećaju na član 8. stav 2. EKLJP u pogledu poštovanja privatnog života. U svojim sudskim praksama SPEU i ESLJP često međusobno upućuju na presude koje donose, što je deo neprekidnog dijaloga između ta dva suda, kako bi se postiglo usklađeno tumačenje propisa o zaštiti podataka. U članu 52. stav 3. Povelje navodi se: „[U]koliko ova povelja sadrži prava koja odgovaraju pravima zajemčenim Konvencijom za zaštitu ljudskih prava i osnovnih sloboda, značenje i obim tih prava su istovetni onima utvrđenim tom konvencijom. ". Međutim, član 8. Povelje ne odgovara sasvim nijednom članu iz EKLJP[81]. Član 52. stav 3. Povelje odnosi se na sadržaj i opseg primene prava zaštićenih pojedinim pravnim poretkom, a ne na uslove njihovog ograničenja. Međutim, s obzirom na širi kontekst dijaloga i saradnje između dvaju sudova, SPEU u svojim analizama može uzeti u obzir kriterijume za zakonito ograničenje na osnovu člana 8. EKLJP-a, u skladu sa tumačenjem ESLJP-a. Moguć je i obrnuti scenario, u kojem ESLJP može upućivati na uslove za zakonito ograničenje na osnovu Povelje. U svakom slučaju, potrebno je uzeti u obzir i da u EKLJP-u ne postoji odreda koja bi bila parnjak članu 8. Povelje i koji bi se odnosio na zaštitu ličnih podataka, a posebno na prava ispitanika, legitimne osnove obrade podataka i nadzor nezavisnog tela. Određeni elementi člana 8. Povelje mogu se pronaći u sudskoj praksi ESLJP-a, razvijenoj na osnovu člana 8. EKLJP-a i u vezi sa Konvencijom br. 108[82]. Ovom vezom se obezbeđuje da SPEU i ESLJP utiču jedan na drugoga u pitanjima u vezi sa zaštitom podataka.

80 *Ibid.*, st. od 56 do 61.

81 EDPS (2017.), *Paket alata za određivanje nužnosti mera*, Bruxelles, 11. aprila 2017, str. 6.

82 Objašnjenja koja se odnose na Povelju Evropske unije o osnovnim pravima (2007/C 303/02), čl. 8.

1.3. Odnos sa drugim pravima i legitimnim interesima

Ključne tačke

- Pravo na zaštitu podataka obično je povezano sa drugim pravima, kao što su sloboda izražavanja i pravo na dobijanje i širenje informacija.
- Taj odnos je često ambivalentan: u nekim slučajevima je pravo na zaštitu ličnih podataka u sukobu s određenim pravom, ali postoje i slučajevi u kojima se pravom na zaštitu ličnih podataka zapravo obezbeđuje poštovanje tog istog prava. Na primer, takav je slučaj sa slobodom izražavanja, budući da je čuvanje poslovne tajne elemenat prava na poštovanje privatnog života.
- Potreba za zaštitom prava i sloboda drugih jedan je od merila prema kojima se procenjuje zakonito ograničenje prava na zaštitu ličnih podataka.
- Kada su različita prava dovedena u pitanje, sudovi moraju da odmere interese kako bi ih uskladili.
- Opštom uredbom o zaštiti podataka propisuje države članice se obavezuju da usklade pravo na zaštitu ličnih podataka sa slobodom izražavanja i informisanja.
- Države članice mogu takođe da donesu određene propise u domaćim zakonodavstvima kako bi uskladile pravo na zaštitu ličnih podataka sa javnim pristupom službenim dokumentima i obavezama čuvanja poslovne tajne.

Pravo na zaštitu ličnih podataka nije apsolutno pravo. Uslovi za zakonito ograničenje tog prava detaljno su objašnjeni u prethodnom delu. Jedan od kriterijuma za zakonito ograničenje prava, priznat i pravom Saveta Evrope i EU, jeste nužnost mešanja u zaštitu podataka radi zaštite prava i sloboda drugih osoba. Kada se zaštita podataka povezuje s drugim pravima, i ESLJP i SPEU su više puta ponovili da je potrebno odmeravanje interesa kada se primenjuju i tumače član 8. EKLJP i član 8. Povelje[83]. Nekoliko važnih primera opisuje kako se postiže ova ravnoteža.

83 ESLJP, *Von Hannover protiv Nemačke* (br. 2) [VV], br. 40660/08 i 60641/08, 7. februara 2012; SEU, spojeni predmeti C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) protiv Administración del Estado*, 24. novembra 2011., stav 48.; SEU, C-275/06, *Productores de Música de España (Promusicae) protiv Telefónica de España SAU* [VV], 29. januara 2008, stav 68.

Pored postupka uravnotežavanja koji vrše ovi sudovi, države mogu po potrebi da usvoje propise kojim bi se pravo na zaštitu ličnih podataka uskladilo s drugim pravima. Zbog toga Opšta uredba o zaštiti podataka omogućava usvajanje niza izuzetaka na domaćem nivou izuzeća.

Kad je reč o slobodi izražavanja, OUZP-om se državama članicama propisuje da zakonom usklade „pravo na zaštitu ličnih podataka, u skladu s ovom Uredbom, s pravom na slobodu izražavanja i informisanja, što uključuje obradu u novinarske svrhe i svrhe akademskog, umetničkog ili književnog izražavanja"[84]. Države članice takođe mogu da donesu zakone za usklađivanje zaštite podataka sa javnim pristupom službenim dokumentima i obavezama čuvanja profesionalne tajne kao jednog oblika poštovanja privatnog života[85].

1.3.1. Sloboda izražavanja

Jedno od prava koje se najviše povezuje s pravom na zaštitu podataka jeste pravo na slobodu izražavanja.

Sloboda izražavanja zaštićena je članom 11. Povelje („Sloboda izražavanja i informisanja"). To pravo obuhvata „slobodu mišljenja kao i primanja i davanja informacija i ideja bez mešanja organa vlasti i bez obzira na granice". U skladu sa članom 11. Povelje i članom 10. EKLJP, slobodom informisanja štiti se pravo ne samo na davanje već i na *primanje* informacija.

Ograničenja slobode izražavanja moraju ispunjavati prethodno opisane kriterijume utvrđene u članu 52. stav 1. Povelje. Osim toga, član 11. odgovara članu 10. EKLJP-a. U skladu sa članom 52. stav 3. Povelje, u meri u kojoj ona sadrži prava koja odgovaraju pravima zagarantovanim EKLJP-om, „značenje i opseg primene tih prava jednaki su onima iz spomenute Konvencije". Ograničenja koja zakonito mogu da se nametnu pravu zagarantovanom u članu 11. Povelje zato ne smeju da premaše ona iz člana 10. stav 2. EKLJP-a. Drugim rečima, moraju da budu zakonom propisana i nužna u demokratskom društvu „radi zaštite [...] ugleda ili prava drugih". Takva prava obuhvataju prvenstveno pravo na poštovanje privatnog života i pravo na zaštitu ličnih podataka.

Odnos između zaštite ličnih podataka i slobode izražavanja regulisan je članom 85. Opšte uredbe o zaštiti podataka naslovljenim „Obrada i sloboda izražavanja i infor-

84 Opšta uredba o zaštiti podataka, član 85.

85 *Ibid.*, članovi 86. i 90.

misanja". Prema tom članu, države članice zakonom usklađuju pravo na zaštitu ličnih podataka s pravom na slobodu izražavanja i informisanja. Konkretno, izuzeća i odstupanja od određenih poglavlja Opšte uredbe o zaštiti podataka uvode se u novinarske svrhe i svrhe akademskog, umetničkog ili književnog izražavanja ako su ona potrebna kako bi se uskladilo pravo na zaštitu ličnih podataka sa slobodom izražavanja i informisanja.

Primer: U predmetu *Tietosuojavaltuutettu protiv Satakunnan Markkinapörssi Oy i Satamedia Oy*[86] od SPEU je zatraženo da definiše odnos između zaštite podataka i slobode štampe[87]. Sud je morao da ispita slučaj objavljivanja poreskih podataka otprilike 1,2 miliona fizičkih lica putem SMS poruka, koje su ove kompanije zakonito dobile od finskih poreskih organa. Finsko nadzorno telo za zaštitu podataka izdalo je odluku kojom se od kompanije traži da prestane da objavljuje te podatke. Kompanija je osporila tu odluku pred domaćim sudom, koji je zatražio obrazloženje SPEU o tumačenju Direktive o zaštiti podataka. SPEU je prvenstveno trebalo da proveri da li treba da se obrada ličnih podataka, koje su poreska tela stavila na raspolaganje kako bi se korisnicima mobilnih telefona omogućilo primanje poreskih podataka drugih fizičkih lica, smatra delatnošću koja se vrši isključivo u novinarske svrhe. Zaključivši da su se delatnosti kompanije sastojale od „obrade ličnih podataka" u smislu člana 3. stav 1. Direktive o zaštiti podataka, SPEU je analizirao član 9. Direktive (o obradi ličnih podataka i slobodi izražavanja). Najpre se osvrnuo na važnost prava na slobodu izražavanja u svakom demokratskom društvu, držeći da pojmovi povezani s tom slobodom, kao što je novinarstvo, treba široko da se tumače. Zatim je napomenuo da se radi postizanja ravnoteže između dvaju osnovnih prava, izuzeća i ograničenja prava na zaštitu podataka moraju primenjivati samo ako je to strogo nužno. U tim okolnostima SPEU je smatrao da se delatnosti kao što su one koje su vršile te dve kompanije, a koje su se ticale podataka iz dokumenata u javnom domenu u okviru domaćeg zakonodavstva, mogu klasifikovati kao „novinarske delatnosti" ako je njihov predmet otkrivanje informacija, mišljenja i ideja javnosti, nezavisno od medija korišćenog za njihov prenos. Takođe je presudio da takve delatnosti nisu ograničene na medijske kompanije i da se

86 SPEU, C-73/07, *Tietosuojavaltuutettu protiv Satakunnan Markkinapörssi Oy i Satamedia Oy* [VV], 16. decembra 2008, st. 56., 61. i 62.

87 Predmet se odnosio na tumačenje člana 9. Direktive o zaštiti podataka, sada zamenjenog članom 85. Opšte uredbe o zaštiti podataka, u kome stoji sledeće: „Države članice utvrđuju izuzetke ili odstupanja od odredbi ovog poglavlja, poglavlja IV i poglavlja V za obradu ličnih podataka izvršenih isključivo u novinarske svrhe ili radi umetničkog ili književnog izražavanja jedino ako su potrebni radi usklađivanja prava na privatnost s propisima o slobodi izražavanja".

mogu obavljati u svrhe sticanja profita. Međutim, SPEU je prepustio domaćem sudu odluku o tome da li je tako bilo u ovom konkretnom slučaju.

Isti predmet je preispitao i ESLJP, nakon što je na osnovu smernica SPEU nacionalni sud odlučio da nalog nadzornog tela da se obustavi objava svih poreskih podataka predstavlja opravdano mešanje u slobodu izražavanja kompanija. ESLJP je podržao takav pristup[88]. Zaključio je da je, uprkos mešanju u pravo na širenje informacija kompanija, mešanje bilo u skladu sa zakonom, njime je nastojano da se ostvari legitiman cilj i bilo je nužno u demokratskom društvu.

Sud je podsetio na merila iz sudske prakse kojima bi domaća tela trebalo da se vode, kao i sam ESLJP, prilikom procene slobode izražavanja i prava na poštovanje privatnog života. Kada su u pitanju politički govor ili debata o nekom pitanju od javnog interesa, malo je prostora za ograničenje prava na dobijanje i širenje informacija, jer javnost ima pravo na informisanje, „a to je osnovno pravo u demokratskom društvu"[89]. Međutim, ne može se smatrati da novinski članci kojima je cilj isključivo da zadovolji radoznalost određenih čitalaca za pojedinostima iz privatnog života neke osobe doprinose raspravi od javnog interesa. Izuzeća od propisa zaštite podataka za novinske svrhe predviđena su da novinarima omoguće pristup podacima, kao i njihovo prikupljanje i obradu kako bi mogli da obavljaju svoje novinarske poslove. Stoga je zaista postojao javni interes za pružanje pristupa velikim količinama poreskih podataka i omogućavanje njihovog prikupljanja i obrade kompanijama, podnosiocima predstavki. S druge strane, ESLJP je zaključio da nije bilo javnog interesa u grupnoj objavi takvih neobrađenih podataka u novinama, u neizmenjenom obliku i bez ikakvih analitičkih radnji. Informacije o oporezivanju mogle su radoznalim građanima da omoguće kategorizovanje pojedinaca prema njihovom ekonomskom statusu i zadovolje radoznalost javnosti za informacijama o privatnim životima drugih osoba. To se nije moglo smatrati doprinosom raspravi od javnog interesa.

Primer: U predmetu *Google Spain*[90] SPEU je razmatrao da li je kompanija Gugl bila obavezna da izbriše zastarele informacije o tužiočevim finansijskim poteškoćama iz popisa rezultata pretraživanja. Kada se tužiočevo ime tražilo

88 ESLJP, *Satakunnan Markkinapörssi Oy i Satamedia Oy protiv Finske* [VV], br. 931/13, 27. juna 2017.

89 *Ibid.*, stav 169.

90 SPEU, C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González* [VV], 13. maja 2014, st. od 81 do 83.

u internet pretraživaču Gugl, rezultati pretrage uključivali su linkove na stare novinske članke u kojima se navodila njegova povezanost sa stečajnim postupkom. Tužilac je to smatrao kršenjem svojih prava na poštovanje privatnog života i zaštitu ličnih podataka budući da je postupak dovršen godinama ranije, pa su takve reference bile nevažne.

SPEU je prvo pojasnio da internet pretraživači i rezultati pretraživanja koji sadrže lične podatke mogu poslužiti za izradu detaljnog profila osobe. S obzirom da društvo postaje sve više digitalizovano, zahtev da lični podaci budu tačni i da njihova objava ne prelazi ono što je nužno, odnosno pružanje informacija javnosti, ključan je za obezbeđivanje visokog nivoa zaštite podataka pojedinaca. „[R]ukovalac podacima u okviru svojih odgovornosti, nadležnosti i mogućnosti [mora] da obezbedi da ta aktivnost zadovoljava uslove" iz prava Unije kako bi predviđene garancije mogle da razviju svoj puni efekat. To znači da pravo na brisanje ličnih podataka kada njihova obrada više nije potrebna ili su oni zastareli, takođe obuhvata internet pretraživače, koji se smatraju i rukovaocima podacima, a ne samo obrađivačima podataka (videti deo 2.3.1).

Prilikom razmatranja da li je Gugl obavezan da ukloni linkove povezane sa tužiocem SPEU je zaključio da u određenim uslovima pojedinci imaju pravo na brisanje svojih ličnih podataka iz rezultata pretraživanja internet pretraživača. Na to pravo se može pozvati kada informacije o nekom pojedincu nisu tačne, dovoljne ili relevantne ili ih je previše za svrhe obrade podataka. SPEU je potvrdio da to pravo nije apsolutno, nego se mora odmeriti u odnosu na druga prava, naročito interes i pravo šire javnosti na pristup tim informacijama. Za svaki zahtev za brisanje potrebna je pojedinačna procena kako bi se uspostavila ravnoteža između osnovnih prava na zaštitu ličnih podataka i privatnog života ispitanika, s jedne strane, i legitimnih interesa svih korisnika interneta, s druge. SPEU je pružio smernice o činiocima koje je potrebno uzeti u obzir prilikom odmeravanja interesa. Priroda tih informacija posebno je važan činilac. Ako su informacije osetljive s obzirom na privatni život pojedinca i ne postoji javno interesovanje za dostupnošću tih informacija, zaštita podataka i privatnost bile bi važnije od prava šire javnosti na pristup informacijama. Nasuprot tome, ako je ispitanik javna ličnost ili su informacije takve da opravdavaju omogućavanje pristupa šire javnosti tim informacijama, tada je mešanje u osnovna prava na zaštitu podataka i privatnost opravdano.

Sledeći tu presudu, Radna grupa iz člana 29. usvojila je smernice o sprovođenju odluke SPEU-a. Smernice sadrže popis uobičajenih merila koje primenjuju

nadzorna tela prilikom obrade tužbi u vezi sa zahtevima pojedinaca za brisanje i kojih bi ona trebalo da se pridržavaju prilikom uravnotežavanja prava[91].

U pogledu usaglašavanja prava na zaštitu podataka i prava na slobodu izražavanja, Evropski sud za ljudska prava doneo je nekoliko značajnih presuda.

Primer: U predmetu *Axel Springer AG protiv Nemačke*[92] ESLJP je smatrao da je zabranom, kojom je kompaniji, podnosiocu predstavke, onemogućeno objavljivanje članka o hapšenju i osudi poznatog glumca, povređen član 10. EKLJP. ESLJP se ponovo pozvao na merila koje je utvrdio u svojoj sudskoj praksi, a koje treba uzeti u obzir prilikom odmeravanja prava na slobodu izražavanja i prava na poštovanje privatnog života:

- da li je događaj na koji se odnosio objavljeni članak bio od opšteg interesa,
- da li je dotična osoba javna ličnost i
- kako su informacije dobijene i da li su bile pouzdane.

ESLJP je utvrdio da su hapšenje i osuda glumca javna sudska činjenica i da su zato od javnog interesa, da je glumac dovoljno poznat da bi se smatrao javnom ličnošću, kao i da su informacije dobijene iz kancelarije javnog tužioca, pa stranke nisu osporavale njihovu tačnost. Zato ograničenja objave nametnuta kompaniji nisu bila opravdano srazmerna legitimnom cilju zaštite privatnog života tužioca. ESLJP je stoga zaključio da je došlo do povrede člana 10. Konvencije.

Primer: Predmet *Coudec i Hachette Filipacchi Associés protiv Francuske*[93] odnosio se na objavu intervjua sa gđom Koste u francuskom nedeljniku, u kojem je ona izjavila da je knez Albert od Monaka otac njenog sina. U intervjuu je takođe opisan odnos gđe Koste sa knezom i način na koji je on reagovao na rođenje deteta, uz fotografije kneza sa detetom. Knez Albert pokrenuo je

91 Radna grupa iz člana 29. (2014), *Guidelines on the implementation of the CJEU judgment on „Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González"* C-131/12 (Smernice o sprovođenju presude Suda Evropske unije u predmetu „Google Spain i Inc protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje Gonzáleza", C-131/12), WP 225, Bruxelles, 26. novembra 2014.

92 ESLJP, *Axel Springer AG protiv Nemačke* [VV], br. 39954/08, 7. februara 2012, st. 90 i 91.

93 ESLJP, *Coudec i Hachette Filipacchi Associés protiv Francuske* [VV], br. 40454/07, 10. novembra 2015.

sudski postupak protiv izdavačke kuće zbog kršenja njegovog prava na zaštitu privatnog života. Francuski sudovi utvrdili su da je objava članka izazvala nepovratnu štetu knezu Albertu pa su naložili izdavaču da plati odštetu i objavi pojedinosti presude na naslovnoj strani časopisa.

Izdavači časopisa pokrenuli su postupak pred ESLJP-om, tvrdeći da su se francuski sudovi neopravdano umešali u njihovo pravo na slobodu izražavanja. ESLJP je trebalo da odmeri pravo kneza Alberta na poštovanje privatnog života s pravom izdavača na izražavanje i pravom šire javnosti na informacije. Pravo gđe Koste da podeli svoju priču s javnošću i interes deteta za službeno utvrđivanje odnosa oca i deteta takođe su bili važni činioci.

ESLJP je smatrao da objava intervjua predstavlja mešanje u privatni život kneza, pa je preispitao da li je mešanje bilo nužno. Utvrdio je da se objava odnosila na javnu ličnost i pitanje od javnog interesa. Budući da su građani Monaka imali interesovanje za saznanjem o postojanju kneževog deteta jer je budućnost nasledne monarhije „neodvojivo povezana s postojanjem potomaka", a što je pitanje od interesa za javnost[94]. Sud je takođe istakao da je članak omogućio gđi Koste i njenom detetu ostvarivanje prava na slobodu izražavanja. Domaći sudovi nisu propisno uzeli u obzir načela i merila razvijene u sklopu sudske prakse ESLJP-a za procenu prava na poštovanje privatnog života i prava na slobodu izražavanja. Na kraju je zaključio da je Francuska prekršila član 10. EKLJP-a po pitanju slobode izražavanja.

U sudskoj praksi ESLJP-a jedno od ključnih merila koji se tiču odmeravanja tih prava je merilo doprinosa datog načina izražavanja raspravi od opšteg javnog interesa.

Primer: U predmetu *Mosley protiv Ujedinjenog Kraljevstva*[95] nacionalni nedeljnik je objavio intimne fotografije podnosioca predstavke, poznate osobe koja je naknadno pokrenula građansku parnicu protiv izdavača, pa joj je dodeljena odšteta. Uprkos ostvarenoj novčanoj naknadi, podnosilac predstavke je tvrdio da je i dalje žrtva kršenja prava na privatnost, jer mu je uskraćena mogućnost da izdejstvuje sudsku zabranu pre objave predmetnih fotografija, budući da ne postoji nikakav zakonski uslov prema kojem bi novine morale da obaveste osobu pre objave.

94 *Ibid*., st. od 104 do 116.

95 ESLJP, *Mosley protiv Ujedinjenog Kraljevstva*, br. 48009/08, 10. maja 2011, st. 129 i 130.

ESLJP je naveo da, iako je navedeni materijal objavljen u načelu više u zabavne nego u obrazovne svrhe, nedvosmisleno se podrazumevala zaštita garantovana članom 10. EKLJP-a tako da se takva objava mogla nadovezati na zahteve iz člana 8. EKLJP-a s obzirom na to da su informacije bile privatne i intimne prirode i da nije bilo javnog interesa za njihovu objavu. Ovde je ipak trebalo obratiti posebnu pažnju pri ispitivanju ograničenja koja se mogu smatrati oblikom cenzure pre objave. U svetlu neprijatnosti koje bi moglo da izazove postavljanje zahteva za prethodnim obaveštavanjem, nedoumica o njegovoj delotvornosti i širokog polja slobodne procene u ovoj oblasti, ESLJP je zaključio da se članom 8. ne zahteva pravno obavezujući zahtev prethodnog obaveštavanja. U skladu s tim, ESLJP je zaključio da nije došlo do povrede člana 8.

Primer: U predmetu *Bohlen protiv Nemačke*[96] podnosilac predstavke, poznati pevač i muzički producent, objavio je autobiografiju iz koje je naknadno morao da ukloni određene odlomke na osnovu sudske presude. Priča je dobila mnogo medijske pažnje u državi, a jedna kompanija za proizvodnju duvanskih proizvoda je pokrenula humorističku marketinšku kampanju upućujući na ovaj događaj, u kojoj je upotrebljeno ime podnosioca predstavke bez njegove dozvole. Podnosilac predstavke je neuspešno zahtevao odštetu od marketinške kompanije, navodeći kršenje svojih prava na osnovu člana 8. EKLJP. ESLJP se pozvao na merila na kojima se zasniva uravnotežavanje prava na poštovanje privatnog života i prava na slobodu izražavanja, pa je zaključio da nije došlo do povrede člana 8. Podnosilac predstavke je bio javna ličnost i u oglasu nisu pomenute pojedinosti iz njegovog privatnog života, nego javno poznat događaj koji je već bio medijski propraćen i koji je činio deo javne rasprave. Usto, oglas je bio humorističke prirode i nije sadržao ništa ponižavajuće ili negativno u vezi sa podnosiocem predstavke.

Primer: U predmetu *Biriuk protiv Litvanije*[97] podnositeljka predstavke je pred ESLJP-om tvrdila da Litvanija nije ispunila svoju obavezu obezbeđivanja poštovanja njenog prava na privatni život jer su joj, uprkos tome što su poznate dnevne novine ozbiljno povredile njenu privatnost, nadležni domaći sudovi koji su ispitivali predmet dodelili zanemarivu novčanu odštetu. Prilikom dodele nenovčane naknade štete, domaći sudovi su primenili odredbe domaćeg zakonodavstva koje se odnose na pružanje informacija javnosti, čime je nametnuta niska gornja granica nenovčane naknade štete zbog nezakonite

96 ESLJP, *Bohlen protiv Nemačke*, br. 53495/09, 19. februara 2015, st. od 45 do 60.

97 ESLJP, *Biriuk protiv Litvanije*, br. 23373/03, 25. novembra 2008.

objave informacija o privatnom životu pojedinca u medijima. Predmet je pokrenut zbog objave članka na naslovnoj strani najvećih dnevnih novina u Litvaniji u kojem je stajalo da je podnositeljka predstavke HIV-pozitivna. U članku je takođe iznesena kritika ponašanja podnositeljke predstavke i dovedene su u pitanje njene moralne vrednosti.

ESLJP je podsetio da je zaštita ličnih podataka, a naročito medicinskih, od ključne važnosti za pravo na poštovanje privatnog života u okviru EKLJP. Poverljivost zdravstvenih podataka posebno je važna s obzirom na to da otkrivanje medicinskih podataka (u ovom slučaju HIV status podnositeljke predstavke) može znatno da utiče na privatni i porodični život osobe, njeno zaposlenje i društvenu uključenost. Sud je posebnu važnost pridao činjenici da je, prema novinskom članku, medicinsko osoblje bolnice objavilo informacije o HIV statusu podnositeljke predstavke i tako jasno prekršilo svoju obavezu čuvanja doktorske tajne. Stoga nije bilo legitimnog mešanja u pravo na njen privatni život.

Članak su objavile novine, a sloboda izražavanja takođe je osnovno pravo prema EKLJP. Međutim, prilikom ispitivanja da li je postojanje javnog interesovanja opravdavalo objavu te vrste podataka o podnositeljki predstavke, ESLJP je zaključio da je glavna svrha njihove objave bilo povećanje prodaje novina podsticanjem radoznalosti čitalaca. Za takvu svrhu se ne može smatrati da doprinosi raspravi od opšteg interesa za društvo. Budući da je ovde bilo reči o „nečuvenoj zloupotrebi slobode štampe", znatna ograničenja u nadoknadi štete i nizak iznos nenovčane naknade obezbeđene domaćim zakonodavstvom značili su da Litvanija nije ispunila svoju pozitivnu obavezu zaštite prava podnositeljke predstavke na privatni život. ESLJP je zaključio da je došlo do povrede člana 8. EKLJP.

Pravo na slobodu izražavanja i pravo na zaštitu ličnih podataka nisu uvek u sukobu. Postoje slučajevi u kojima se efikasnom zaštitom ličnih podataka garantuje sloboda izražavanja.

Primer: SPEU je u predmetu *Tele2 Sverige* utvrdio da je mešanje u osnovna prava utvrđena u članovima 7. i 8. Povelje, prouzrokovano Direktivom 2006/24 (Direktiva o zadržavanju podataka), bilo „široko i treba da se smatra naročito teškim. Dalje, okolnost da se zadržavanje i naknadno korišćenje podataka izvršava bez obaveštavanja pretplatnika ili registrovanog korisnika može kod dotičnih osoba [...] stvoriti osećaj da je njihov privatni život predmet neprekidnog

nadzora". SPEU je takođe zaključio da je opšte zadržavanje podataka o potrošnji i lokaciji moglo da utiče na korisničku upotrebu elektronske komunikacije i „stoga na uživanje njihove slobode izražavanja zagarantovane u članu 11. Povelje"[98]. U tom smislu, zahtevanjem da se stroge zaštitne mere za zadržavanje podataka ne sprovode na uopšten način propisi za zaštitu podataka doprinose uživanju slobode izražavanja.

Kad je reč o pravu na primanje informacija, koje je takođe deo slobode izražavanja, sve je snažnija spoznaja o važnosti transparentnosti vlasti za funkcionisanje demokratskog društva. Transparentnost je cilj od opšteg interesa kojim bi se zato moglo opravdati mešanje u pravo na zaštitu podataka, ako je to potrebno i srazmerno, kao što je objašnjeno u delu 1.2. U skladu s tim, u poslednje dve decenije je pravo pristupa dokumentima javnih tela potvrđeno kao važno pravo svakog građanina EU, kao i svakog fizičkog lica koje boravi odnosno pravnog lica sa sedištem u nekoj državi članici.

U okviru prava Saveta Evrope može se upućivati na načela sadržana u Preporuci o pristupu službenim dokumentima koja je nadahnula autore Konvencije o pristupu službenim dokumentima (Konvencija br. 205)[99].

U okviru prava Unije pravo na pristup dokumentima zagarantovano je Uredbom br. 1049/2001 o javnom pristupu dokumentima Evropskog parlamenta, Saveta i Komisije (Uredba o pristupu dokumentima)[100]. Članom 42. Povelje i članom 15. stav 3. Ugovora u funkcionisanju Evropske unije to pravo na pristup je prošireno na pristup „dokumentima institucija, tela, kancelarija i agencija Unije nezavisno od njihovog oblika".

To pravo može biti u suprotnosti sa pravom na zaštitu podataka ako se pristupom dokumentu otkrivaju lični podaci pojedinca. Članom 86. Opšte uredbe o zaštiti podataka jasno se utvrđuje da tela javne vlasti i druga tela mogu da otkriju lične podatke

98 SPEU, spojeni predmeti C-203/15 i C-698/15, *Tele2 Sverige AB protiv Post- och telestyrelsen i Secretary of State for the Home Department protiv Toma Watsona i drugih* [VV], 21. decembra 2016, st. 37. i 101.; SPEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr.* i *Kärntner Landesregierung i dr.* [VV], 8. aprila 2014, stav 28.

99 Savet Evrope, Savet ministara (2002), Preporuka R (81) 19 i Preporuka Rec(2002)2 državama članicama o pristupu službenim dokumentima, 21. februara 2002; Savet Evrope, Konvencija o pristupu službenim dokumentima, CETS br. 205, 18. juna 2009. Konvencija još nije stupila na snagu.

100 Uredba (EZ) br. 1049/2001 Evropskog parlamenta i Saveta od 30. maja 2001. o javnom pristupu dokumentima Evropskog parlamenta, Saveta i Komisije, SL 2001 L 145.

iz službenih dokumenata koje poseduju u skladu sa pravom Unije[101] ili pravom države članice kako bi se uskladio javni pristup službenim dokumentima s pravom na zaštitu ličnih podataka u skladu s Uredbom.

Stoga može da bude potrebno da se uravnoteže zahtevi za pristup dokumentima ili informacijama javnih tela s pravom na zaštitu podataka osoba čiji su podaci sadržani u zatraženim dokumentima.

Primer: U predmetu *Volker und Markus Schecke i Hartmut Eifert protiv Land Hessen*[102], SPEU je morao da proceni srazmernost objave imena korisnika poljoprivrednih subvencija Evropske unije i iznosa koje je svaki od njih primio, kako nalaže zakonodavstvo EU. Objavljivanjem takvih informacija nastojalo se da se poveća transparentnost i doprinese javnoj kontroli administracije u pogledu odgovarajuće upotrebe javnih sredstava. Nekoliko korisnika je osporilo srazmernost takve objave.

Napominjući da pravo na zaštitu podataka nije apsolutno pravo, SPEU je smatrao da je objava podataka o imenima korisnika dvaju poljoprivrednih fondova Unije, sa ukupnim iznosima primljenih novčanih pomoći na internet stranici, zadiranje u privatni život korisnika, a naročito u zaštitu njihovih ličnih podataka.

SPEU je smatrao da je takvo zadiranje u članove 7. i 8. Povelje omogućeno zakonom, kao i da je njime ispunjen cilj od opšteg interesa koji EU priznaje, tj. transparentnije korišćenje fondova zajednice. Uprkos tome, SPEU je smatrao da je objava imena fizičkih lica korisnika poljoprivredne subvencije EU iz spomenuta dva fonda, i ukupnih iznosa koje su primili, nesrazmerna i neopravdana mera uzimajući u obzir član 52. stav 1. Povelje. SPEU je naglasio važnost obaveštavanja poreskih obveznika o upotrebi javnih sredstava u demokratskom društvu. Međutim, s obzirom na to da „nije moguće uopšte priznati nikakav automatski prioritet cilja transparentnosti nad pravom zaštite ličnih podataka"[103], institucije EU morale su da odmere interese transparentnosti Unije sa ograničenjem ostvarivanja prava na privatnost i zaštitu podataka koje su korisnici doživeli zbog objave.

101 Član 42. Povelje, član 15. stav 3. UFEU-a i Uredbe br. 1049/2009.

102 SPEU, spojeni predmeti C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen* [VV], 9. novembra 2010, st. od 47 do 52, 58, 66, 67, 75, 86 i 92.

103 *Ibid.*, stav 85.

SPEU je smatrao da institucije EU nisu pravilno odmerile te interese, jer je bilo moguće zamisliti mere koje bi manje štetno uticale na osnovna prava pojedinaca, a istovremeno deotvorno doprinele cilju transparentnosti koji je nastojao da se ostvari objavom. Na primer, umesto opšte objave koja se odnosi na sve korisnike, s njihovim imenom i tačnim iznosima koje je svaki od njih primio, mogla se napraviti razlika na osnovu relevantnih kriterijuma kao što su periodi u kojima su te osobe primile subvenciju, učestalost subvencije ili njeni iznosi i obeležja[104]. Sud je stoga zakonodavstvo Evropske unije o objavi informacija o korisnicima evropskih poljoprivrednih fondova proglasio delimično nevažećim.

Primer: U predmetu *Rechnungshof protiv Österreichischer Rundfunk i dr.*[105] SPEU je preispitao usklađenost određenih austrijskih zakona sa zakonodavstvom EU o zaštiti podataka. Zakonom je bilo propisano da državno telo prikuplja i šalje podatke o prihodu u svrhu objave imena i prihoda zaposlenih raznih javnih tela u okviru godišnjeg izveštaja dostupnog široj javnosti. Neke osobe su odbile da daju svoje podatke pozivajući se na zaštitu podataka.

SPEU se u svom mišljenju oslonio na zaštitu osnovnih prava kao opšteg načela prava Unije i na član 8. EKLJP-a, napominjući da Povelja u tom trenutku nije bila obavezujuća. Smatrao je da prikupljanje podataka o prihodu od rada pojedinca, a naročito njihovo prenošenje trećim stranama, spada u oblast primene prava na poštovanje privatnog života i predstavlja kršenje tog prava. Mešanje se moglo opravdati da je bilo u skladu sa zakonom, da je njime nastojano da se ostvari legitiman cilj i da je bilo nužno u demokratskom društvu radi ostvarenja tog cilja. SPEU je istakao da je austrijskim zakonom nastojao da se ostvari legitiman cilj, jer je taj cilj bio održavanje plata javnih službenika u okvirima razumnih ograničenja, što je povezano sa ekonomskom dobrobiti države. Međutim, interes Austrije u obezbeđenju optimalnog iskorišćavanja javnih sredstava morao je da se uporedi sa ozbiljnošću mešanja u pravo dotičnih osoba na poštovanje njihovog privatnog života.

Iako je SPEU prepustio domaćem sudu da utvrdi da li je objava podataka o prihodu pojedinaca bila nužna i srazmerna cilju koji je nastojano da se ostvari zakonom, pozvao je domaći sud da razmotri da li se takav cilj mogao ostvariti podjednako delotvorno na manje nametljiv način. Jedan od primera bi bio prenos ličnih podataka samo nadzornim javnim telima, a ne široj javnosti.

104 *Ibid.*, stav 89.

105 SPEU, spojeni predmeti C-465/00, C-138/01 i C-139/01, *Rechnungshof protiv Österreichischer Rundfunk i dr. i Christa Neukomm i Joseph Lauermann protiv Österreichischer Rundfunk*, 20. maja 2003.

U kasnijim predmetima postalo je jasno da uravnotežavanje zaštite podataka i pristupa dokumentima zahteva podrobnu analizu pojedinih slučajeva. Nijedno pravo ne može automatski poništiti drugo. SPEU je u dva predmeta imao priliku da tumači pravo na pristup dokumentima koji sadrže lične podatke.

Primer: U predmetu *Evropska komisija protiv Bavarian Lager*[106] SPEU je definisao oblast primene zaštite ličnih podataka u kontekstu pristupa dokumentima institucija EU i odnos između uredbi br. 1049/2001 (Uredba o pristupu dokumentima) i br. 45/2001 (Uredba o zaštiti podataka u institucijama EU). Kompanija Bavarian Lager, osnovana 1992. godine, uvozi nemačko pivo u bocama u Ujedinjeno Kraljevstvo, prvenstveno za pivnice i barove. Međutim, navedena kompanija je naišla na prepreke, jer je britansko zakonodavstvo *de facto* u povoljniji položaj stavljalo domaće proizvođače. Kao odgovor na žalbu kompanije Bavarian Lager, Evropska komisija odlučila je da pokrene postupak protiv Ujedinjenog Kraljevstva jer nije ispunila svoju obavezu, nakon čega su izmenjene osporavane odredbe koje su usklađene sa pravom Unije. Bavarian Lager je zatim od Komisije, pored ostalih dokumenata, zatražio i kopiju zapisnika sa sastanka u kome su učestvovali predstavnici Komisije, britanskih nadležnih tela i udruženja *Confédération des Brasseurs du Marché Commun* (CBMC). Komisija je pristala da otkrije određena dokumenta u vezi sa sastankom, ali izostavila je pet imena koja su se pojavljivala u zapisniku, jer su se dve osobe izričito protivile otkrivanju identiteta, a Komisija nije uspela da kontaktira ostala tri učesnika. Odlukom od 18. marta 2004. Komisija je odbila novi zahtev društva Bavarian Lager za integralni zapisnik sa sastanka pozivajući se prvenstveno na zaštitu privatnog života pojedinaca zagarantovanu Uredbom o zaštiti podataka u institucijama EU.

Budući da nije bila zadovoljna iznesenim stavom, kompanija Bavarian Lager podnela je tužbu Prvostepenom sudu. Taj sud je poništio odluku Komisije presudom od 8. novembra 2007. godine (predmet T-194/04, *The Bavarian Lager Co. Ltd. protiv Komisije Evropskih zajednica*), smatrajući da samo navođenje imena dotičnih osoba koje su predstavljale određena tela na popisu učesnika sastanka ne predstavlja narušavanje privatnog života, niti dovodi privatne živote tih osoba u bilo kakvu opasnost.

106 SPEU, C-28/08 P, *Evropska komisija protiv The Bavarian Lager Co. Ltd* [VV], 29. juna 2010.

Po žalbi Komisije SPEU je poništio presudu Prvostepenog suda. SPEU je smatrao da se Uredbom o pristupu dokumentima utvrđuje „poseban i pojačan sistem zaštite osobe čiji bi se lični podaci mogli, zavisno od slučaja, otkriti javnosti". Prema SPEU, kada se zahtevom koji se zasniva na Uredbi o pristupu dokumentima traži pristup dokumentima koji uključuju lične podatke, u celini se primenjuju odredbe Uredbe o zaštiti podataka u institucijama EU. SPEU je zatim zaključio da je Komisija s pravom odbila zahtev za pristup celovitom sadržaju zapisnika sa sastanka iz oktobra 1996. U nedostatku dozvole petoro učesnika sastanka, Komisija je u dovoljnoj meri ispunila svoju dužnost otvorenosti dostavljajući verziju dokumenta u kojoj su izostavljena njihova imena.

Štaviše, prema SPEU, „kako Bavarian Lager nije izričito i legitimno opravdao svoj zahtev, niti je pružio ikakav uverljiv argument kojim bi dokazao nužnost dostave tih ličnih podataka, Komisija nije mogla da odmeri razne interese dotičnih stranaka, niti je mogla da proveri da li je bilo razloga za pretpostavku da se mogu ugroziti legitimni interesi ispitanika", kako se zahteva Uredbom o zaštiti podataka u institucijama EU-a.

Primer: U predmetu *ClientEarth i Pesticide Action Network Europe (PAN Europe) protiv Evropske agencije za bezbednost hrane (EFSA)*[107] SPEU je ispitao da li je odluka Evropske agencije za bezbednost hrane (EFSA) o uskraćivanju punog pristupa dokumentima tužiocima bila nužna za zaštitu prava na privatnost i zaštitu podataka osoba na koje se u dokumentima upućivalo. Dokumenta su se odnosila na nacrt izveštaja o smernicama koji je pripremila radna grupa EFSA-e u saradnji sa inostranim stručnjacima u vezi sa stavljanjem fitosanitarnih proizvoda na tržište. EFSA je prvobitno dozvolila delimičan pristup tužiocima i uskratila pristup određenim radnim verzijama nacrta dokumenta sa smernicama. Posle toga dozvolila je pristup nacrtu koji je uključivao pojedinačne komentare inostranih stručnjaka. Međutim, izostavila je imena stručnjaka pozivajući se na član 4. stav 1. tačka (b) Uredbe br. 45/2001 o obradi ličnih podataka u institucijama i telima EU kao i na potrebu za zaštitom privatnosti inostranih stručnjaka. U prvostepenoj presudi Opšti sud EU potvrdio je EFSA-inu odluku.

Posle žalbe tužilaca, SPEU je poništio prvostepenu presudu. Zaključio je da je prenos ličnih podataka u tom slučaju bio nužan za utvrđivanje nepristrasnosti svakog od inostranih stručnjaka u njihovom obavljanju naučnih dužnosti, kao i

107 SPEU, C-615/13P, *ClientEarth i Pesticide Action Network Europe (PAN Europe) protiv Evropske agencije za sigurnost hrane (EFSA) i Evropske komisije*, 16. jula 2015.

za obezbeđivanje transparentnosti postupka donošenja odluka u EFSA-i. Prema SPEU, EFSA nije navela kako bi otkrivanje imena inostranih stručnjaka, koji su sastavili pojedine komentare o nacrtu dokumenta sa smernicama, uticalo na legitimne interese tih stručnjaka. Opšti argument da otkrivanje imena može da naruši privatnost nije dovoljan ako nije potkrepljen dokazima specifičnim za svaki pojedini slučaj.

Prema ovim presudama, za mešanje u pravo na zaštitu podataka u kontekstu pristupa dokumentima potreban je određen i opravdan razlog. Pravom na pristup dokumentima ne može se automatski isključiti pravo na zaštitu podataka[108].

Taj pristup je sličan pristupu ESLJP-a u pogledu privatnosti i pristupa dokumentima, kao što pokazuje sledeća presuda. U presudi *Magyar Helsinki* ESLJP je naveo da se članom 10. pojedincima ne dodeljuje pravo na pristup informacijama koje imaju javna tela, niti obavezuje vlasti na pružanje takvih informacija pojedincima. Međutim, takvo pravo ili obaveza može se pojaviti prvenstveno kada je otkrivanje informacija propisano sudskim nalogom koji je dobio pravnu snagu, zatim kada je pristup informacijama ključan za ostvarivanje prava pojedinca na slobodu izražavanja, a naročito slobodu dobijanja i širenja informacija, kao i kada bi se njihovim uskraćivanjem mešalo u to pravo[109]. Da li i u kojoj meri uskraćivanje pristupa informacijama predstavlja mešanje u slobodu izražavanja pojedinca mora se proceniti u svakom pojedinačnom slučaju i u kontekstu njegovih posebnih okolnosti, uključujući sledeće: (i) svrhu zahteva za informacije; (ii) prirodu informacija koje se traže; (iii) ulogu tužilaca i (iv) spremnost i dostupnost informacija.

Primer: U predmetu *Magyar Helsinki Bizottság protiv Mađarske*[110] podnosilac predstavke, nevladina organizacija za zaštitu ljudskih prava, zatražio je informacije od policije u vezi sa radom branilaca po službenoj dužnosti za završetak istraživanja o funkcionisanju sistema javnih pravobranilaca u Mađarskoj. Policija je odbila da pruži te informacije, tvrdeći da su one lični podaci koji ne podležu objavljivanju. Primenjujući navedena merila, ESLJP je smatrao da je došlo do mešanja u pravo zaštićeno članom 10. Tačnije, podnosilac

108 Međutim, videti detaljne rasprave u EDPS (2011.), *Public access to documents containing personal data after the Bavarian Lager ruling* (Javni pristup dokumentima koji sadrže lične podatke posle presude u predmetu Bavarian Lager), Bruxelles, 24. marta 2011.

109 ESLJP, *Magyar Helsinki Bizottság protiv Mađarske* [VV], br. 18030/11, 8. novembra 2016, stav 148.

110 *Ibid*., st. 181, od 187 do 200.

predstavke je hteo da iskoristi pravo na širenje informacija o pitanju od javnog interesa, tražio je pristup informacijama u tu svrhu, pa su informacije bile nužne za njegovo uživanje prava na slobodu izražavanja. Informacije o imenovanju javnih pravobranilaca bile su od interesa za javnost. Nije bilo razloga za sumnju da je navedeno istraživanje uključivalo informacije koje je podnosilac predstavke nameravao da objavi i koje je javnost imala pravo da dobije. Sud je zato zaključio da je pristup traženim informacijama bio nužan da bi podnosilac predstavke ispunio zadatak. Na kraju, informacije su bile spremne i dostupne.

ESLJP je zaključio da je uskraćivanjem pristupa informacijama u tom slučaju narušena suština slobode dobijanja informacija. U svrhu donošenja takvog zaključka, razmotrio je posebno svrhu zatraženih informacija i njihov doprinos važnoj javnoj raspravi, prirodu traženih informacija i njihov potencijalni javni interes, kao i položaj koji je podnosilac predstavke u ovom predmetu imao u društvu.

Sud je u obrazloženju napomenuo da se istraživanje koje je sprovela NVO odnosilo na rad pravosuđa i pravo na pravično suđenje, što je jedno od prava izuzetnog značaja prema EKLJP. Budući da zatražene informacije nisu uključivale podatke izvan javnog domena, prava privatnosti ispitanika (branilaca po službenoj dužnosti) ne bi bila narušena da je policija podnosiocu predstavke odobrila pristup informacijama. Informacije koje je podnosilac predstavke zatražio bile su statistički podaci u vezi sa brojem slučajeva u kojima su branioci po službenoj dužnosti bili imenovani radi zastupanja optuženih u javnim krivičnim postupcima.

Budući da se istraživanjem nastojalo da se doprinese važnoj raspravi o pitanju od opšteg interesa, ESLJP je smatrao da su sva ograničenja predložene studije NVO-a trebala da se podvrgnu podrobnoj proveri. Predmetne informacije bile su od javnog interesa s obzirom na to da javni interes obuhvata „pitanja koja mogu da prouzrokuju znatne kontroverze, pitanja koja se odnose na važan društveni problem ili pitanja koja uključuju problem koji bi mogao da bude od interesa za javnost"[111]. Stoga bi svakako obuhvatao raspravu pravosuđu i pravičnim postupcima, što je bilo predmet istraživanja podnosioca predstavke. Odmeravanjem različitih prava i primenom načela srazmernosti, ESLJP je zaključio da je došlo do neopravdanog kršenja prava podnosioca predstavke prema članu 10. EKLJP.

111 *Ibid*., stav 156.

1.3.2. Poslovna tajna

Prema domaćem pravu, određene komunikacije mogu da podležu obavezi čuvanja poslovne tajne. Poslovna tajna može se protumačiti kao posebna etička dužnost koja podrazumeva pravnu obavezu svojstvenu određenim strukama i funkcijama koje se temelje na pouzdanosti i poverenju. Osobe i institucije koje obavljaju te funkcije obavezne su da čuvaju poverljive podatke koje dobiju prilikom obavljanja svojih dužnosti. Poslovna tajna prvenstveno se povezuje s medicinskom strukom i poverljivošću komunikacije između advokata i klijenta, a mnoge jurisdikcije priznaju obavezu čuvanja poslovne tajne i u finansijskom sektoru. Poslovna tajna nije osnovno pravo, ali zaštićena je kao oblik prava na poštovanje privatnog života. Na primer, SPEU je presudio da u određenim slučajevima postoji „potreba za zabranom otkrivanja određenih informacija koje su proglašene poverljivima u svrhu očuvanja osnovnog prava preduzetnika na poštovanje privatnosti, kako je utvrđeno u članu 8. EKLJP i članu 7. Povelje"[112]. ESLJP je takođe odlučivao o tome da li ograničenja poslovne tajne predstavljaju povredu člana 8. EKLJP, kako je opisano u sledećim istaknutim primerima.

Primer: U predmetu *Pruteanu protiv Rumunije*[113] podnosilac predstavke je postupao kao advokat trgovačke kompanije kojoj je bilo zabranjeno izvršavanje bankovnih transakcija nakon optužbi za prevaru. Tokom razmatranja predmeta rumunski sudovi su odobrili tužilaštvu da presretne i snima telefonske razgovore partnera kompanije tokom određenog perioda. Snimci i presretnuti razgovori uključivali su komunikaciju s njegovim advokatom.

Gospodin Pruteanu je tvrdio da to predstavlja mešanje u njegovo pravo na poštovanje privatnog života i prepiske. ESLJP je u presudi istakao status i važnost odnosa advokata s klijentom. Presretanjem razgovora advokata s klijentom nedvosmisleno je prekršena poslovna tajna, koja čini osnovu odnosa između tih dveju osoba. U takvom slučaju advokat takođe može da se žali na mešanje u njegovo pravo na poštovanje privatnog života i prepiske. SPEU je smatrao da je povređen član 8. EKLJP-a.

112 SPEU, predmet T-462/12 R, *Pilkington Group Ltd protiv Evropske komisije*, Rešenje predsednika Opšteg suda, 11. marta 2013, stav 44.

113 ESLJP, *Pruteanu protiv Rumunije*, br. 30181/05, 3. februara 2015.

Primer: U predmetu *Brito Ferrinho Bexiga Villa-Nova protiv Portugalije*[114] podnositeljka predstavke, inače advokatica, odbila je da otkrije svoje lične bankovne izvode poreskim organima na osnovu poslovne i bankovne tajne. Kancelarija tužioca pokrenula je istragu zbog poreske prevare i zatražio je odobrenje za privremeno ukidanje poslovne tajne. Domaći sudovi izdali su nalog za privremeno ukidanje pravila poverljivosti i bankovne tajne, zaključivši da bi javni interes trebalo da prevagne nad ličnim interesima podnositeljke predstavke.

Kada je predmet došao do ESLJP-a, on je smatrao da je pristup bankovnim izvodima podnositeljke predstavke predstavljao mešanje u njeno pravo na poštovanje poslovne tajne, koje je obuhvaćeno konceptom privatnog života. Mešanje je imalo pravnu osnovu jer se zasnivalo na zakoniku o krivičnom postupku i njime je nastojano da se ostvari legitiman cilj. Međutim, preispitujući nužnost i srazmernost mešanja, ESLJP je istakao činjenicu da je postupak za ukidanje poverljivosti sproveden bez učešća ili znanja podnositeljke predstavke. Ona stoga nije mogla da iznese svoje argumente. Usto, iako je domaćim zakonodavstvom propisano da je u takvom postupku potrebno savetovanje s advokatskom komorom, ono nije sprovedeno. Na kraju, podnositeljka predstavke nije imala mogućnost da delotvorno ospori ukidanje poverljivosti, niti je imala na raspolaganju bilo kakav pravni lek kojim bi osporila tu meru. Zbog izostanka regulatornih garancija i delotvornog sudskog nadzora nad merom kojom se obustavlja dužnost čuvanja poverljivosti, ESLJP je zaključio da je došlo do povrede člana 8. EKLJP.

Odnos između poslovne tajne i zaštite podataka često ima dva značenja. S jedne strane, propisi i mere za zaštitu podataka utvrđeni zakonodavstvom pomažu u očuvanju poslovne tajne. Na primer, propisima kojima se rukovaoci podacima i obrađivači podataka obavezuju na uvođenje strogih mera za bezbednost podataka nastoji se, između ostalog, da se spreči gubitak poverljivosti ličnih podataka zaštićenih poslovnom tajnom. Zatim, Opštom uredbom EU o zaštiti podataka omogućava se obrada zdravstvenih podataka koji čine posebne kategorije ličnih podataka, za koje je potrebna snažnija zaštita, ali oni istovremeno podležu uspostavljanju primerenih i posebnih mera zaštite prava ispitanika, a naročito poslovne tajne[115].

114 ESLJP, *Brito Ferrinho Bexiga Villa-Nova protiv Portugalije*, br. 69436/10, 1. decembra 2015.

115 Opšta uredba o zaštiti podataka, član 9. stav 2. tačka (h) i član 9. stav 3.

S druge strane, obavezama poslovne tajne nametnutim rukovaocima podacima i obrađivačima podataka u pogledu određenih ličnih podataka mogu se ograničiti prava ispitanika, a posebno pravo na dobijanje informacija. Iako Opšta uredba o zaštiti podataka sadrži opsežan popis informacija koje u načelu moraju da se daju ispitaniku ako lični podaci nisu dobijeni od njega, taj zahtev objave ne primenjuje se kada lični podaci moraju da ostanu poverljivi zbog obaveze poslovne tajne propisane nacionalnim zakonodavstvom ili zakonodavstvom EU[116].

Opštom uredbom o zaštiti podataka (OUZP) omogućava se da države članice donesu posebne zakonske propise za zaštitu obaveze poslovne tajne ili druge obaveze tajnosti iste vrednosti i da usklade pravo na zaštitu ličnih podataka sa obavezom poslovne tajne[117].

OUZP propisuje da države članice mogu doneti posebne propise o ovlašćenjima nadzornih tela u vezi sa rukovaocima podacima ili obrađivačima podataka koji imaju obavezu čuvanja poslovne tajne. Ti posebni propisi povezani su s ovlašćenjem ostvarivanja pristupa poslovnom prostoru rukovaoca podacima ili obrađivača podataka, njihovoj opremi za obradu podataka i ličnim podacima koje poseduju, ako su takvi lični podaci dobijeni u okviru aktivnosti obuhvaćene obavezom tajnosti. Zato nadzorna tela nadležna za zaštitu podataka moraju da poštuju obaveze poslovne tajne koje se odnose na rukovaoca podacima i obrađivača podataka. Zatim, i članovi nadzornih tela imaju dužnost čuvanja poslovne tajne tokom i posle svog mandata. U izvršavanju svojih zadataka članovi i osoblje nadzornih tela mogu saznati određene poverljive informacije. Članom 54. stav 2. Uredbe jasno se propisuje da imaju dužnost da čuvaju poslovne tajne u pogledu takvih poverljivih informacija.

OUZP od država članica zahteva da obaveste Komisiju o pravilima koja donesu radi usklađivanja zaštite podataka i načela utvrđenih Uredbom sa obavezom čuvanja poslovne tajne.

1.3.3. Sloboda veroispovesti i uverenja

Sloboda veroispovesti i uverenja zaštićena je članom 9. EKLJP (sloboda mišljenja, savesti i veroispovesti) i članom 10. Povelje EU o osnovnim pravima. Lični podaci koji otkrivaju verska i filozofska uverenja smatraju se „osetljivim podacima" prema pravu EU i Saveta Evrope tako da njihova obrada i upotreba podležu pojačanoj zaštiti.

116 *Ibid*., član 14. stav 5. tačka (d).

117 *Ibid*., uvodna izjava 164 i član 90.

Primer: Podnosilac predstavke u predmetu *Sinak Işık protiv Turske*[118] bio je član verske zajednice alevita, čija su verovanja pod uticajem sufizma i drugih predislamskih verovanja i koju neki akademski stručnjaci smatraju zasebnom religijom, a drugi delom islamske veroispovesti. Podnosilac predstavke se žalio da je njegova lična karta suprotno njegovim željama sadržala polje u kojem je njegova veroispovest označena kao „islam" umesto „alevizam". Domaći sudovi su odbili njegov zahtev za promenu unosa na ličnoj karti u „alevizam" uz obrazloženje da ta reč označava podgrupu islama, a ne zasebnu religiju. Zatim je podneo predstavku pred ESLJP-om u kojoj je naveo da je bio prisiljen da javno obznani svoju veroispovest bez odobrenja, jer je navođenje veroispovesti na ličnoj karti bilo obavezno, tako da je time prekršeno njegovo pravo na slobodu veroispovesti i savesti, naročito kad se uzme u obzir da oznaka „islam" na ličnoj karti nije bila tačna.

ESLJP je ponovio da sloboda veroispovesti podrazumeva slobodu izražavanja veroispovesti u zajednici s drugim osobama, u javnosti kao i u krugu ljudi koji pripadaju istoj veroispovesti, kao i u privatnosti i kada je osoba sama. Prema tadašnjem domaćem pravu pojedinci su bili obavezni da imaju ličnu kartu, dokument na kojem je naznačena njihova veroispovest, koju je trebalo pokazati na zahtev bilo kog javnog organa ili privatnog preduzeća. U sklopu te obaveze nije uzeto u obzir da se pravom izražavanja veroispovesti podrazumeva i suprotno pravo, odnosno pravo na oslobađanje od obaveze objave veroispovesti. Iako je vlada tvrdila da je domaće zakonodavstvo izmenjeno kako bi pojedinci mogli da zatraže da polje o veroispovesti na ličnoj karti ostane prazno, prema mišljenju ESLJP, sama činjenica da je potrebno podneti zahtev da se stavka veroispovesti izbriše može predstavljati otkrivanje informacija o stavu prema religiji. Usto, kada lične karte imaju polje o veroispovesti, njegovo ostavljanje praznim ima specifično značenje, jer bi vlasnici ličnih karata bez informacija o veroispovesti bili izdvojenimeđu onima na čijoj je ličnoj karti ta stavka navedena. ESLJP je zaključio da se domaćim pravom krši član 9. EKLJP-a.

Međutim, za rad crkvi i verskih udrženja ili zajednica može biti potrebna obrada ličnih podataka članova, kako bi se omogućila komunikacija i organizacija aktivnosti unutar zajednice vernika. Zato crkve i verska udrženja često uvode pravila obrade ličnih podataka. Prema članu 91. Opšte uredbe o zaštiti podataka, kada su takva

118 ESLJP, *Sinan Işık protiv Turske*, br. 21924/05, 2. februara 2010.

pravila sveobuhvatna, mogu i dalje biti važeća pod uslovom da se usklade s odredbama Uredbe. Crkve i verska udruženja koje imaju takva pravila moraju se podvrgnuti nadzoru nezavisnog nadzornog tela, koje može da bude posebno nadležno za njih, pod uslovom da ispunjava uslove Opšte uredbe o zaštiti podataka za takva tela[119].

Verske organizacije mogu da obrađuju lične podatke iz nekoliko razloga, na primer, radi održavanja kontakta s vernicima ili prenošenja informacija o verskim ili dobrotvornim događajima i proslavama koje organizuju. U određenim državama crkve moraju da vode spiskove članova zbog poreskih razloga, budući da broj članova verskih ustanova može da utiče na iznos poreza koje pojedinci treba da plaćaju. U svakom slučaju, prema evropskom pravu, podaci koji otkrivaju religijska uverenja pojedinaca smatraju se osetljivim podacima i crkve moraju da snose odgovornost za rukovanje takvim podacima i njihovu obradu, naročito s obzirom na to da se informacije koje obrađuju verske organizacije često odnose na decu, starije osobe ili druge osetljive grupe u društvu.

1.3.4. Sloboda umetnosti i nauke

Sloboda umetnosti i nauke, koja je izričito zaštićena članom 13. Povelje EU o osnovnim pravima, predstavlja još jedno pravo koje treba odmeriti u odnosu na prava na poštovanje privatnog života i zaštitu podataka. To pravo je u prvom redu izvedeno iz prava na slobodu mišljenja i izražavanja, a njegovo ostvarivanje podleže članu 1. Povelje (ljudsko dostojanstvo). ESLJP smatra da je sloboda umetnosti zaštićena članom 10. Evropske konvencije o ljudskim pravima[120]. Pravo zagarantovano članom 13. Povelje može da podleže i ograničenjima iz člana 52. stav 1. Povelje, koji se može tumačiti i iz perspektive člana 10. stav 2. EKLJP-a[121].

Primer: U predmetu *Vereinigung bildender Künstler protiv Austrije*[122] austrijski sudovi zabranili su udruženju, podnositeljki predstavke, dalje izlaganje slike s fotografijama glava različitih javnih ličnosti u seksualnim pozama. Poslanik austrijskog parlamenta, čija je fotografija takođe iskorišćena na slici, pokrenuo je postupak protiv udruženja, tražeći zabranu izlaganja slike. Domaći sud je izrekao zabranu. ESLJP je ponovio da se član 10. EKLJP-a primenjuje na širenje ideja koje vređaju, izazivaju šok ili uznemiravaju državu ili bio koji deo populacije.

119 Opšta uredba o zaštiti podataka, član 91. stav 2.

120 ESLJP, *Müller i drugi protiv Švajcarske*, br. 10737/84, 24. maja 1988.

121 Objašnjenja koja se odnose na Povelju Evropske unije o osnovnim pravima, SL 2007 C 303.

122 ESLJP, *Vereinigung bildender Künstler protiv Austrije*, br. 68354/01, 25. januara 2007, st. 26. i 34.

Oni koji stvaraju, izvode, šire ili izlažu umetnička dela doprinose razmeni ideja i mišljenja i država je dužna da im ne uskrati nepotrebno slobodu izražavanja. Budući da je predmetna slika bila kolaž u kome su iskorišćene samo glave osoba, a njihova tela su oslikana na nerealističan i preteran način, čija svrha očigledno nije bila predstavljanje pa čak ni nagoveštaj stvarnosti, ESLJP je zatim izjavio da se „slika teško može tumačiti kao da se tiče privatnog života [dotičnog], već se ona pre tiče njegovog javnog položaja političara" i da je „u tom svojstvu [dotični] trebalo da pokaže više tolerancije na kritiku". Odmeravajući različite interese, ESLJP je zaključio da je neograničena zabrana daljeg izlaganja slike nesrazmerna. ESLJP je stoga zaključio da je došlo do povrede člana 10. Konvencije.

Evropsko zakonodavstvo o zaštiti podataka uzima u obzir i posebnu vrednost koju nauka ima za društvo. Opštom uredbom o zaštiti podataka i modernizovanom Konvencijom br. 108 dopušta se zadržavanje podataka tokom dužih perioda ako će se lični podaci upotrebljavati isključivo u svrhu naučnih ili istorijskih istraživanja. Zatim, nezavisno o izvornoj svrsi određene aktivnosti obrade, dalja upotreba ličnih podataka u naučnim istraživanjima ne smatra se neprikladnom svrhom[123]. Istovremeno se moraju sprovesti odgovarajuće zaštitne mere za takvu obradu kako bi se zaštitila prava i slobode ispitanika. U pravu EU ili država članica mogu se propisati izuzeci od prava ispitanika, na primer prava na pristup, ispravku, ograničenje obrade i prigovor u vezi s obradom njihovih ličnih podataka u svrhu naučnih istraživanja i u istorijske ili statističke svrhe (videti i deo 6.1. i deo 9.4).

1.3.5. Zaštita intelektualne svojine

Pravo na zaštitu svojine sadržano je u članu 1. Prvog protokola uz Evropsku konvenciju o ljudskim pravima i u članu 17. stav 1. Povelje EU o osnovnim pravima. Jedan od aspekata prava na svojinu koji je posebno značajan za zaštitu podataka jeste zaštita intelektualne svojine, koja se izričito spominje u članu 17. stav 2. Povelje. U pravnom poretku EU postoji nekoliko direktiva donesenih u svrhu efikasne zaštite intelektualne svojine i to naročito autorskog prava. Intelektualna svojina ne obuhvata samo literarnu i umetničku svojinu, već i patente, žigove i srodna prava.

Iz sudske prakse SPEU jasno proizlazi da se zaštita osnovnog prava na svojinu mora uravnotežiti sa zaštitom drugih osnovnih prava, naročito prava na zaštitu poda-

123 Opšta uredba o zaštiti podataka, član 5. stav 1. tačka (b) i modernizovana Konvencija br. 108, član 5. stav 4. tačka (b).

taka[124]. Bilo je slučajeva kada su institucije za zaštitu autorskih prava od pružalaca usluga pristupa internetu tražile da otkriju identitet korisnika internet platformi za zajedničko korišćenje datoteka. Takve platforme, naime, korisnicima interneta često omogućavaju besplatno preuzimanje muzičkih zapisa uprkos tome što su zaštićeni autorskim pravom.

Primer: Predmet *Promusicae protiv Telefónica de España*[125] odnosio se na protivljenje španskog pružaoca usluga pristupa internetu, kompanije Telefónica, otkrivanju ličnih podataka nekolicine osoba kojima je pružao usluge pristupa internetu neprofitnoj organizaciji muzičkih producenata i izdavača muzičkih i audiovizuelnih snimaka pod nazivom Promusicae. Organizacija Promusicae zatražila je otkrivanje informacija kako bi mogla da pokrene građanski postupak protiv tih osoba, za koje je tvrdila da su upotrebljavale program razmene datoteka s pristupom fonogramima na koje su pravo upotrebe polagali članovi Promusicae.

Španski sud se obratio SPEU, zatraživši odgovor na pitanje da li, prema pravu Zajednice, takvi lični podaci moraju da se saopšte u kontekstu građanskih parnica kako bi se obezbedila delotvorna zaštita autorskog prava. Pozvao se na direktive 2000/31, 2001/29 i 2004/48, tumačene i u kontekstu članova 17. i 47. Povelje. Sud je zaključio da te tri direktive, kao i Direktiva o privatnosti i elektronskim komunikacijama (Direktiva 2002/58), ne sprečavaju države članice da propišu obavezu otkrivanja ličnih podataka u kontekstu građanskih parnica, radi delotvorne zaštite autorskog prava.

SPEU je istakao da je slučaj podstakao pitanje potrebe za usklađivanjem zahteva za zaštitu različitih osnovnih prava, odnosno prava na poštovanje privatnog života sa pravom na zaštitu svojine i na delotvoran pravni lek.

Zaključio je da „države članice kod prenošenja navedenih direktiva moraju da brinu o tome da ih tumače na način koji omogućava obezbeđivanje pravične ravnoteže između različitih osnovnih prava koja su zaštićena pravnim poretkom Zajednice. Zatim, prilikom sprovođenja mera za prenošenje navedenih direktiva, na telima i sudovima država članica jeste dužnost ne samo da svoje domaće pravo tumače u skladu sa tim direktivama, nego i da ih ne tumače na način koji

124 SPEU, C-275/06, *Productores de Música de España (Promusicae) protiv Telefónica de España SAU* [VV], 29. januara 2008, st. od 62. do 68.

125 *Ibid*., st. 54. i 60.

bi bio protivan navedenim osnovnim pravima ili drugim opštim načelima prava Zajednice, kao što je načelo srazmernosti"[126].

Primer: Predmet *Bonnier Audio AB i drugi protiv Perfect Communication Sweden AB*[127] odnosio se na ravnotežu između prava intelektualne svojine i zaštite ličnih podataka. Tužioci – pet izdavačkih kuća koje su bile nosioci autorskih prava na 27 audio-knjiga – pokrenuli su postupak pred švedskim sudom, navodeći da su ta autorska prava prekršena putem FTP servera (protokola za prenos podataka koji omogućava deljenje datoteka i prenos podataka putem interneta). Tužioci su od pružaoca usluga interneta (PUI) zatražili da otkrije ime i adresu osobe koja je koristila IP adresu sa koje su poslate datoteke. Pružalac usluga, kompanija ePhone, osporila je taj zahtev, navodeći da se njime krši Direktiva 2006/24 (Direktiva o zadržavanju podataka, proglašena nevažećom 2014).

Švedski sud se obratio SPEU uz pitanje da li Direktiva 2006/24 sprečava primenu domaće odredbe koja se zasniva na članu 8. Direktive 2004/48 (Direktiva o sprovođenju prava intelektualne svojine), kojim se omogućava izdavanje sudskog naloga kojim se zahteva da PUI prenesu informacije nosiocima autorskih prava o pretplatnicima čije su IP adrese navodno upotrebljene za kršenje prava. To pitanje se zasnivalo na pretpostavci da je tužilac izneo jasne dokaze o kršenju određenog autorskog prava i da je mera srazmerna.

SPEU je istakao da se Direktiva 2006/24 odnosi isključivo na rukovanje podacima i zadržavanje podataka koje proizvedu pružaoci elektronskih komunikacionih usluga u svrhu istrage, otkrivanja i gonjenja teških krivičnih dela kao i na njihovo prenošenje nadležnim nacionalnim telima. Zato se domaća odredba kojom se Direktiva o sprovođenju prava intelektualne svojine prenosi u domaće zakonodavstvo nalazi izvan područja primene Direktive 2006/24 i stoga nije onemogućena Direktivom[128].

Kad je reč o prenosu imena i adrese koje su tražili tužioci, SPEU je smatrao da takav postupak predstavlja obradu ličnih podataka i pripada oblasti primene Direktive 2002/58 (Direktiva o privatnosti i elektronskim komunikacijama). Takođe je napomenuo da je prenos takvih podataka potrebno u građanskim

126 *Ibid*., st. 65. i 68; videti i SPEU, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) protiv Netlog NV*, 16. februara 2012.

127 SPEU, C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB protiv Perfect Communication Sweden AB*, 19. aprila 2012.

128 *Ibid*., st. 40. i 41.

parnicama, kako bi se nosiocu autorskih prava obezbedila delotvorna zaštita autorskih prava, pa zato zbog svoje svrhe takođe pripada oblasti primene Direktive 2004/48[129].

SPEU je zaključio da direktive 2002/58 i 2004/48 moraju da se tumače tako da ne sprečavaju domaće zakonodavstvo, poput onoga koje se navodi u glavnom postupku, da nacionalnom sudu, koji odlučuje o zahtevu za izdavanje naloga za otkrivanje ličnih podataka, omogući odmeravanje sukobljenih interesa, na osnovu činjenica svakog pojedinog slučaja i uzimajući u obzir zahteve načela srazmernosti.

1.3.6. Zaštita podataka i ekonomski interesi

U doba digitalnih tehnologija ili velikih podataka, podaci se nazivaju „novom naftom" jer podstiču ekonomske inovacije i kreativnost[130]. Mnoge kompanije su izgradile snažne poslovne modele na obradi podataka, koji obično uključuje lične podatke. Određene kompanije smatraju da pojedina pravila u vezi sa zaštitom ličnih podataka u praksi mogu da prouzrokuju preopterećenje obavezama koje mogu utcati na njihove ekonomske interese. Zato se postavlja pitanje da li ekonomski interesi rukovalaca podacima i obrađivača podataka ili šire javnosti mogu da opravdaju ograničavanje prava na zaštitu podataka.

Primer: U predmetu *Google Spain*[131] SPEU je smatrao da u određenim uslovima pojedinci imaju pravo da zatraže da internet pretraživači uklone rezultate pretraživanja iz svojih indeksa za traženje. U svom obrazloženju SPEU je istakao činjenicu da se upotrebom internet pretraživača i navedenih rezultata pretraživanja može utvrditi detaljan profil pojedinca. Te informacije mogu da se odnose na brojne aspekte privatnog života osobe i ne mogu se jednostavno pronaći ili povezati bez internet pretraživača. Takvi postupci zato čine potencijalno ozbiljno mešanje u osnovna prava na privatnost i zaštitu ličnih podataka ispitanika.

129 *Ibid.*, st. od 52. do 54. Videti i SEU, C-275/06, *Productores de Música de España (Promusicae) protiv Telefónica de España SAU* [VV], 29. januara 2008., stav 58.

130 Na primer, videti *Financial Times* (2016.), „Data is the new oil... who's going to own it?", 16. novembra 2016.

131 SPEU, C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González* [VV], 13. maja 2014.

SPEU je zatim ispitao da li se to mešanje može opravdati. U pogledu ekonomskog interesa kompanije, vlasnika internet pretraživača, za obradu podataka, SPEU je naveo: „jasno je da [mešanje] ne može biti opravdano samo ekonomskim interesom operatera takvog pretraživača u toj obradi" i da „po pravilu" osnovna prava iz članova 7. i 8. Povelje imaju prevagu nad takvim ekonomskim interesom i nad interesom javnosti u vezi sa pronalaženjem navedene informacije prilikom pretrage imena ispitanika[132].

Jedno od ključnih pitanja evropskog prava zaštite podataka jeste davanje veće kontrole pojedincima nad sopstvenim ličnim podacima. U digitalnom dobu je posebno prisutna neravnoteža između ovlašćenja poslovnih subjekata, koji obrađuju podatke i imaju pristup znatnim količinama ličnih podataka, i ovlašćenja pojedinaca, kojima ti lični podaci pripadaju, da kontrolišu sopstvene podatke. SPEU svakom predmetu pristupa pojedinačno kada odmerava zaštitu podataka i ekonomske interese, kao što su interesi trećih strana u vezi sa deoničkim društvima i društvima s ograničenom odgovornošću, kao što je vidivo u presudi u predmetu *Manni*.

Primer: Predmet *Manni*[133] odnosio se na uvrštavanje ličnih podataka pojedinca u javni trgovački registar. G. Manni zatražio je od Ekonomske komore grada Leće u Italiji da izbriše njegove lične podatke iz tog registra nakon što je otkrio da bi mogući klijenti pretraživali registar i saznali da je bio upravnik kompanije koja je proglasila stečaj pre više od decenije. Te informacije su uticale na mišljenje njegovih mogućih klijenata i mogle su negativno da se odraze na njegove komercijalne interese.

Od SPEU se tražilo da utvrdi da li se pravom EU priznaje pravo na brisanje u tom slučaju. U donošenju zaključka SPEU je odmerio propise EU o zaštiti podataka i komercijalne interese g. Manija za uklanjanjem informacija o stečaju njegove prethodne kompanije s javnim interesom za pristup tim informacijama. SPEU je uzeo u obzir činjenicu da je objava u javnom registru trgovačkih kompanija propisana zakonom, a naročito direktivom EU kojoj je svrha da učini podatke o kompanijama dostupnijim trećim stranama. Objava je važna radi zaštite interesa trećih strana koje žele da posluju s određenom kompanijom, budući da je jedina zaštitna mera koju akcionarska društva i društva s ograničenom

132 *Ibid.*, st. 81 i 97.

133 SPEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce protiv Salvatorea Mannija*, 9. marta 2017.

odgovornošću pružaju trećim stranama njihova imovina. Stoga „bi osnovni dokumenti trgovačke kompanije trebalo da budu objavljeni kako bi treće strane mogle da provere njihove sadržaje i druge informacije koje se odnose na trgovačku kompaniju, posebno pojedinosti o osobama koje su ovlašćene da obavežu trgovačku kompaniju"[134].

S obzirom na važnost legitimnog cilja koji je nastojao da se postigne registrom, SPEU je smatrao da g. Mani nije imao pravo na brisanje svojih ličnih podataka budući da je potreba za zaštitom interesa trećih strana u odnosu na akcionarska društva i društva s ograničenom odgovornošću, kao i za obezbeđenjem pravne sigurnosti, poštenog poslovanja i pravilnog funkcionisanja unutrašnjeg tržišta, imala prednost nad njegovim pravima na osnovu zakonodavstva o zaštiti podataka. To je posebno tačno kada se u obzir uzme činjenica da su pojedinci koji odluče da učestvuju u trgovini putem akcionarskog društva ili društva s ograničenom odgovornošću svesni da moraju da otkriju podatke o svom identitetu i funkcijama.

Iako je zaključio da nije bilo osnove za brisanje podataka u ovom slučaju, SPEU je priznao da postoji pravo na prigovor na obradu, tvrdeći da „se ne može isključiti mogućnost postojanja određenih situacija u kojima jaki i zakoniti razlozi u vezi s konkretnim slučajem predmetne osobe izuzetno opravdavaju ograničavanje pristupa ličnim podacima koji se na nju odnose, upisanih u registar, po isteku dovoljno dugog roka [...] trećim osobama koje imaju konkretan interes za uvid u njih"[135].

SPEU je utvrdio da je na domaćim sudovima da, uzimajući u obzir sve relevantne okolnosti pojedinca, u svakom predmetu procene postojanje ili nepostojanje zakonitih i jakih razloga kojima bi se izuzetno opravdalo ograničenje pristupa trećih strana ličnim podacima sadržanima u registrima trgovačkih kompanija. Međutim, SPEU je pojasnio da se u slučaju g. Manija činjenica da je otkrivanje njegovih ličnih podataka u registru navodno uticalo na njegove klijente sama po sebi ne može smatrati takvim zakonitim i jakim razlogom. Mogući klijenti g. Manija imaju zakonit interes za informacije o stečaju njegove prethodne kompanije.

134 *Ibid*., stav 49.

135 *Ibid*., stav 60.

Mešanje u osnovna prava g. Manija i drugih osoba uvršćenih u registar na poštovanje privatnog života i zaštitu ličnih podataka, zagarantovana članovima 7. i 8. Povelje, poslužilo je cilju od opšteg interesa tako da je bilo nužno i srazmerno.

Stoga je u predmetu *Manni* SPEU zaključio da prava na zaštitu podataka i privatnost nisu prevagnula nad interesom trećih strana za pristup informacijama u registru trgovačkih kompanija koje se odnose na akcionarska društva i društva s ograničenom odgovornošću.

2 Terminologija zaštite podataka

EU	Obuhvaćena pitanja	Savet Evrope
Lični podaci		
Opšta uredba o zaštiti podataka, član 4. stav 1. Opšta uredba o zaštiti podataka, član 4. stav 5. i član 5. stav 1. tačka (e) Opšta uredba o zaštiti podataka, član 9. SPEU, spojeni predmeti C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen* [VV], 2010. SPEU, C-275/06, *Productores de Música de España (Promusicae) protiv Telefónica de España SAU* [VV], 2008. SPEU, C-70/10, *Scarlet Extended SA protiv Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011. SPEU, C-582/14, *Patrick Breyer protiv Bundesrepublik Deutschland*, 2016. SPEU, spojeni predmeti C-141/12 i C-372/12, *Y. S. protiv Minister voor Immigratie, Integratie en Asiel i Minister voor Immigratie, Integratie en Asiel protiv M. i S.*, 2014.	**Pravna definicija zaštite podataka**	Modernizovana Konvencija br. 108, član 2. tačka (a) ESLJP, *Bernh Larsen Holding AS i drugi protiv Norveške*, br. 24117/08, 2013. ESLJP, *Uzun protiv Nemačke*, br. 35623/05, 2010. ESLJP, *Amann protiv Švajcarske* [VV], br. 27798/95, 2000.
SPEU, C-101/01, *Krivični postupak protiv Bodil Lindqvist*, 2003.	**Posebne kategorije ličnih podataka (osetljivi podaci)**	Modernizovana Konvencija br. 108, član 6. stav 1.

EU	Obuhvaćena pitanja	Savet Evrope
SPEU, C-434/16, *Peter Nowak protiv Data Protection Commissioner*, 2017.	**Anonimi-zovani i pseudo-nimizovani lični podaci**	Modernizovana Konvencija br. 108, član 5. stav 4 .tačka (e) Izveštaj sa objašnjenjima o modernizovanoj Konvenciji br. 108, stav 50
Obrada podataka		
Opšta uredba o zaštiti podataka, član 4. stav 2. SPEU, C-212/13, *František Ryneš protiv Úřad pro ochranu osobních údajů*, 2014. SPEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce protiv Salvatorea Mannija*, 2017. SPEU, C-101/01, *Krivični postupak protiv Bodil Lindqvist*, 2003. SPEU, C-131/12, *Google Spain SL i Google Inc. Protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje Gonzáleza* [VV], 2014.	**Definicije**	Modernizovana Konvencija br. 108, član 2. tačke (b) i (c)
Korisnici podataka		
Opšta uredba o zaštiti podataka, član 4. stav 7. SPEU, C-212/13, *František Ryneš protiv Úřad pro ochranu osobních údajů*, 2014. SPEU, C-1318/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje Gonzáleza* [VV], 2014.	**Rukovalac podacima**	Modernizovana Konvencija br. 108, član 2. tačka (d) Profiling Recommendation (Preporuka o izradi profila), član 1. tačka (g)*
Opšta uredba o zaštiti podataka, član 4. stav 8.	**Obrađivač podataka**	Modernizovana Konvencija br. 108, član 2. tačka (f) Preporuka o izradi profila, član 1. tačka (h)
Opšta uredba o zaštiti podataka, član 4. stav 9.	**Primalac**	Modernizovana Konvencija br. 108, član 2. tačka (e)
Opšta uredba o zaštiti podataka, član 4. stav 10.	**Treća strana**	

EU	Obuhvaćena pitanja	Savet Evrope
Dozvola		
Opšta uredba o zaštiti podataka, član 4. stav 11. i član 7. SPEU, C-543/09, *Deutsche Telekom AG protiv Bundesrepublik Deutschland*, 2011. SPEU, C-536/15, *Tele2 (Netherlands) BV i dr. protiv Autoriteit Consument en Markt (ACM)*, 2017.	**Definicije i zahtevi za važeću dozvolu**	Modernizovana Konvencija br. 108, član 5. stav 2. Medical Data Recommendation (Preporuka o medicinskim podacima), član 6. i razne dalje preporuke ESLJP, *Elberte protiv Latvije*, br. 61243/08, 2015.

*Napomena: * Savet Evrope, Savet ministara (201.), Preporuka CM/Rec(2010)13 državama članicama o zaštiti pojedinaca u vezi s automatskom obradom ličnih podataka u kontekstu izrade profila (Preporuka o izradi profila), 23. novembra 2010.*

2.1. Lični podaci

Ključne tačke

- Podaci su lični ako se odnose na osobu utvrđenog identiteta ili osobu čiji identitet može da se utvrdi, odnosno „ispitanika".
- Kako bi se odredilo da li identitet pojedinca može da se utvrdi, rukovalac podacima ili bilo koja druga osoba trebalo bi da uzme u obzir sva sredstva, kao što je izdvajanje, koja po svemu sudeći mogu da se upotrebe u svrhu neposrednog ili posrednog utvrđivanja identiteta pojedinca.
- Autentifikacija/potvrđivanje je postupak dokazivanja da određena osoba ima određeni identitet i/ili je ovlašćena za preduzimanje određenih radnji.
- Postoje posebne kategorije podataka, takozvani osetljivi podaci, navedeni u modernizovanoj Konvenciji br. 108 i u pravu zaštite podataka EU, koji zahtevaju pojačanu zaštitu i zato podležu posebnom pravnom režimu.
- Podaci su anonimizovani/izostavljeni ako se više ne odnose na osobu utvrđenog identiteta ili osobu čiji se identitet može utvrditi.
- Pseudonimizacija/zamena je mera prema kojoj se lični podaci ne mogu pripisati ispitaniku bez dodatnih informacija, koje se čuvaju odvojeno. „Ključ" koji omogućava ponovnu identifikaciju ispitanika mora se čuvati odvojeno i na bezbednom. Podaci nad kojima je izvršen postupak pseudonimizacije/zamene ostaju lični podaci. U pravu EU ne postoji koncept „pseudonimizovanih podataka".
- Načela i pravila zaštite podataka ne primenjuju se na anonimizovane/izostavljene podatke, ali primenjuju se na pseudonimizovane/zamenjene podatke.

2.1.1. Glavni aspekti koncepta ličnih podataka

Na osnovu prava EU kao i **na osnovu prava Saveta Evrope**, „lični podaci" definisani su kao informacije koje se odnose na identifikovano fizičko lice ili fizičko lice koja može da se identifikuje[136]. „Lični podaci" se odnose na informacije o osobi čiji je identitet sasvim jasan ili ga je barem moguće utvrditi uz dodatne informacije. Kako bi se odredilo može li se identitet pojedinca utvrditi, rukovalac podacima ili bilo koja druga osoba mora uzeti u obzir sva sredstva koja su pogodna za svrhu neposrednog ili posrednog utvrđivanja identiteta pojedinca, kao što je na primer selekcija/izdvajanje, koja omogućava da se s jednom osobom postupa drugačije od drugih[137].

Ako se podaci o takvoj osobi obrađuju, ona se naziva „ispitanik" odnosna osoba na koju se podaci odnose.

Ispitanik

Na osnovu prava EU, fizička lica su jedini korisnici propisa za zaštitu podataka[138] i samo su živa bića zaštićena evropskim zakonodavstvom o zaštiti podataka[139]. U Opštoj uredbi o zaštiti podataka (OUZP) lični podaci se definišu kao svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi.

U pravu Saveta Evrope, posebno u modernizovanoj Konvenciji br. 108, takođe se upućuje na zaštitu pojedinaca u pogledu obrade njihovih ličnih podataka. I u njoj lični podaci označavaju sve podatke koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi. To fizičko lice ili pojedinac, kako se naziva u OUZP-u odnosno modernizovanoj Konvenciji br. 108, u zakonodavstvu o zaštiti podataka poznata je kao ispitanik.

Pravna lica takođe imaju pravo na određenu zaštitu. Postoji sudska praksa ESLJP-a sa presudama po predstavkama pravnih lica zbog navodnih povreda njihovog prava na zaštitu od upotrebe njihovih podataka u skladu sa članom 8. EKLJP-a. Članom 8. EKLJP-a obuhvaćeni su pravo na poštovanje privatnog i porodičnog života, kao i pravo na poštovanje doma i prepiske. Sud stoga može da razmatra predmete u okviru potonjeg, a ne u okviru privatnog života.

---

136 Opšta uredba o zaštiti podataka, član 4. stav 1.; modernizovana Konvencija br. 108, član 2. tačka (a).

137 Opšta uredba o zaštiti podataka, uvodna izjava 26.

138 *Ibid*., član 1.

139 *Ibid*., uvodna izjava 27. Videti i Radna grupa iz člana 29. (2007.), *Mišljenje 4/2007 o konceptu ličnih podataka*, WP 136, 20. juna 2007, str. 22.

Primer: Predmet *Bernh Larsen Holding AS i drugi protiv Norveške*[140] odnosio se na žalbu tri norveške kompanije na odluku poreskog organa koji im je nalagao da poreskim revizorima dostave kopije svih podataka sa računarskog servera koji su zajednički upotrebljavale.

ESLJP je smatrao da je takva obaveza nametnuta kompanijama, podnosiocima predstavki, predstavljala mešanje u njihova prava na poštovanje „doma" i „prepiske" iz člana 8. EKLJP-a. Međutim, ESLJP je zaključio da su poreski organi raspolagali odgovarajućim i delotvornim mehanizmima zaštite od zloupotrebe: kompanije, podnosioci predstavke, obaveštene su dovoljno unapred, bile su prisutne i mogle su da učestvuju u postupku tokom intervencije na licu mesta, a materijal je trebalo uništiti po završetku poreske revizije. U tim okolnostima je postignuta pravična ravnoteža između prava kompanija, podnosilaca predstavki, na poštovanje „doma" i „prepiske" i njihovog interesa u zaštiti privatnosti njihovih zaposlenih, s jedne strane, i javnog interesa delotvorne inspekcije radi poreske procene, s druge strane. ESLJP je zaključio da stoga nije došlo do povrede člana 8.

Prema modernizovanoj Konvenciji br. 108, zaštita podataka u prvom redu se bavi zaštitom fizičkih lica, ali ugovorne strane u okviru domaćeg zakonodavstva mogu proširiti zaštitu podataka i na pravna lica, na primer preduzeća i udruženja. U Izveštaju sa objašnjenjima o modernizovanoj Konvenciji br. 108 navodi se da se domaćim zakonodavstvom mogu zaštititi legitimni interesi pravnih lica proširivanjem oblasti primene Konvencije na takva lica[141]. **Pravo zaštite podataka EU** ne obuhvata obradu ličnih podataka koji se tiču pravnih lica, a naročito preduzeća koja su osnovanakao pravna lica, uključujući ime i oblik pravnog lica i kontakt podatke pravnog lica[142]. Međutim, Direktivom o privatnosti i elektronskim komunikacijama štite se poverljivost komunikacija i legitimni interesi pravnih lica u pogledu povećanja kapaciteta automatskog čuvanja i obrade podataka povezanih s pretplatnicima i korisnicima[143]. Slično tome, nacrtom Uredbe o e-privatnosti zaštita se proširuje na pravna lica.

140 ESLJP, *Bernh Larsen Holding AS i drugi protiv Norveške,* br. 24117/08, 14. marta 2013. Vidi i ESLJP, *Liberty i drugi protiv Ujedinjenog Kraljevstva*, br. 58243/00, 1. jula 2008.

141 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 30.

142 Opšta uredba o zaštiti podataka, uvodna izjava 14.

143 Direktiva o privatnosti i elektronskim komunikacijama, uvodna izjava 7 i član 1. stav 2.

Primer: U predmetu *Volker und Markus Schecke i Hartmut Eifert protiv Land Hessen*[144] SPEU je, pozivajući se na objavu ličnih podataka o korisnicima poljoprivredne pomoći, smatrao da se „pravna lica mogu pozvati na zaštitu iz članova 7. i 8. Povelje samo ako službeni ime/naziv pravnog lica upućuje na jedno ili više fizičkih lica. [...P]oštovanje prava na privatni život s obzirom na obradu ličnih podataka, koje je priznato članovima 7. i 8. Povelje, odnosi se na svaku informaciju koja se tiče fizičkog lica čiji je identitet utvrđen ili se može utvrditi [...]"[145].

Procenom interesa EU da obezbedi transparentnost u dodeli subvenciju, s jedne strane, i osnovnih prava na privatnost i zaštitu podataka pojedinaca koji koriste subvencije, s druge strane, SPEU je zaključio da je mešanje u ta osnovna prava bilo nesrazmerno. SPEU je smatrao je da je cilj transparentnosti mogao delotvorno da se ostvari merama koje su manje nametljive u pogledu prava dotičnih pojedinaca. Međutim, prilikom razmatranja srazmernosti objave informacija o pravnim licima koja su dobila pomoć, SPEU je došao do drugačijeg zaključka, presudivši da takvom objavom nisu prekoračena ograničenja načela srazmernosti. Utvrdio je da se „ozbiljnost povrede prava na zaštitu ličnih podataka iskazuje na različite načine za pravna lica, s jedne strane, i fizičkog lica, s druge"[146]. Pravna lica podležu strožim obavezama u vezi sa objavom informacija o njima. SPEU je smatrao da bi se zahtevanjem da domaća tela ispitaju da li se u podaci svakog pravnog lica, korisnika pomoći, nalaze podaci na osnovu kog se može identifikovati bilo koje povezano fizičko lica, pre objave podataka tim telima, nametnulo nerazumno administrativno opterećenje. Stoga je zakonodavstvom kojim se zahteva opšta objava podataka o pravnim licima uspostavljena pravedna ravnoteža između navedenih sukobljenih interesa.

Priroda podataka

Svaka informacija može biti lični podatak pod uslovom da se odnosi na identifikovanu osobu ili osobu koja se može identifikovati.

144 SPEU, spojeni predmeti C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen* [VV], 9. novembra 2010, stav 53.

145 *Ibid*., st. 52 i 53.

146 *Ibid*., stav 87.

Primer: Procena radnih sposobnosti radnika koju nadređeni pohranjuje u lični dosije radnika predstavlja lični podatak o radniku. To je slučaj čak i ako podaci sadrže, delimično ili u celini, samo lično mišljenje nadređenog, na primer: „radnik nije posvećen poslu", a ne konkretne činjenice kao što je: „radnik je u proteklih šest meseci izostao s posla pet nedelja".

Lični podaci obuhvataju informacije koje se tiču privatnog života osobe, što uključuje i profesionalne aktivnosti, kao i informacije o njenom javnom životu.

U predmetu *Amann*[147] ESLJP je pojam „lični podaci" tumačio ne ograničavajući ga na pitanja privatne sfere pojedinca. To je značenje pojma „lični podaci" takođe bitno za OUZP.

Primer: U predmetu *Volker und Markus Schecke i Hartmut Eifert protiv Land Hessen*[148] SPEU je izjavio da „u tom pogledu činjenica da se objavljeni podaci odnose na profesionalnu delatnost nema uticaja [...]. Evropski sud za ljudska prava odlučio je u odnosu na ovu tačku, u vezi s tumačenjem člana 8. Konvencije [EKLJP], da se pojam ‚privatni život' ne sme tumačiti restriktivno i da ne postoji načelni razlog koji bi opravdao isključivanje delatnosti profesionalne [...] prirode iz pojma ‚privatni život'".

Primer: U spojenim predmetima *Y. S. protiv Minister voor Immigratie, Integratie en Asiel* i *Minister voor Immigratie, Integratie en Asiel protiv M. i S.*[149] SPEU je utvrdio da pravna analiza sadržana u nacrtu odluke Službe za imigraciju i naturalizaciju, koja obrađuje zahteve za dozvolu boravka, sama po sebi ne predstavlja lične podatke, iako može da sadrži određene lične podatke.

Sudska praksa ESLJP-a koja se odnosi na član 8. EKLJP-a potvrđuje kako može da bude teško potpuno razdvojiti pitanja iz privatnog i profesionalnog života[150].

147 Videti ESLJP, *Amann protiv Švajcarske,* br. 27798/95, 16. februara 2000, stav 65.

148 SPEU, spojeni predmeti C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen* [VV], 9. novembra 2010, stav 59.

149 SPEU, spojeni predmeti C-141/12 i C-372/12, *Y. S. protiv Minister voor Immigratie, Integratie en Asiel i Minister voor Immigratie, Integratie en Asiel protiv M. i S.*, 17. jula 2014, stav 39.

150 Videti, na primer, ESLJP, Rotaru protiv Rumunije [VV], br. 28341/95, 4. maja 2000, stav 43.; ESLJP, *Niemietz protiv Nemačke*, br. 13710/88, 16. decembra 1992, stav 29.

Primer: U predmetu *Bărbulescu protiv Rumunije*[151] podnosilac predstavke je otpušten jer je upotrebljavao poslodavčevu internet vezu tokom radnog vremena i time prekršio interna pravila. Njegov poslodavac je nadzirao njegovu komunikaciju i tokom postupka pred domaćim sudom predočeni su zapisi njegovih poruka čisto privatne prirode. ESLJP je utvrdio da je član 8. primenjiv u ovom slučaju i ostavio je otvorenim pitanje da li je na osnovu ograničavajućih pravila poslodavca podnosilac predstavke mogao razumno da očekuje privatnost, ali u svakom slučaju je zaključio da poslodavac svojim uputstvima ne može sasvim da onemogući privatni društveni život na radnom mestu. Kad je reč o osnovanosti takvog postupka, državama ugovornicama moralo se omogućiti široko polje slobodne procene prilikom ocenjivanja potrebe za uspostavljanjem pravnog okvira kojim se uređuju uslovi u kojima poslodavac može da kontroliše neposlovnu komunikaciju zaposlenih na radnom mestu, bilo elektronsku ili neku drugu. Uprkos tome, domaća tela morala su da obezbede da poslodavčevo uvođenje mera za nadziranje dopisivanja i drugih komunikacija, nezavisno od opsega i trajanja takvih mera, bude propraćeno odgovarajućim i dovoljnim zaštitnim merama protiv zloupotrebe. Srazmernost i regulatorne garancije protiv proizvoljnog postupanja bili su od ključne važnosti, a ESLJP je utvrdio niz činilaca koji su bili relevantni u tim okolnostima. Na primer, takvi činioci su uključivali meru u kojoj poslodavac nadzire zaposlene, nivo zadiranja u privatnost zaposlenih, posledice po zaposlene i postojanje odgovarajućih zaštitnih mera. Usto, domaća tela morala su da obezbede da zaposleni, čije se komunikacije nadgledaju, ima pristup pravnom leku pred pravosudnim organom s nadležnošću da utvrdi, barem u suštini, kako se ti navedeni kriterijumi poštuju i da li su sporne mere zakonite. U ovom slučaju ESLJP je utvrdio da je došlo do povrede člana 8. jer domaća tela nisu omogućila odgovarajuću zaštitu prava podnosioca predstavke na poštovanje njegovog privatnog života i prepiske, pa stoga nisu uspostavila pravičnu ravnotežu između predmetnih interesa.

Na osnovu prava EU kao i **prava Saveta Evrope**, informacije sadrže podatke o osobi:

- ako se pojedinac identifikuje ili ga je moguće identifikovati na osnovu tih informacija ili

151 ESLJP, *Bărbulescu protiv Rumunije* [VV], br. 61496/08, 5. septembra 2017, stav 121.

- ako se pojedinac, uprkos tome što nije identifikovan, može selektovati/izdvojiti na osnovu tih informacija na način koji omogućava otkrivanje ispitanika dodatnim istraživanjem.

Obe vrste informacija su na isti način zaštićene evropskim pravom zaštite podataka. Mogućnost direktne ili indirektne identifikacije zahteva neprekidnu procenu „uzimajući u obzir i tehnologiju dostupnu u vreme obrade i tehnološki razvoj"[152]. Evropski sud za ljudska prava često je ponavljao da je pojam „ličnih podataka" prema EKLJP-u isti kao u Konvenciji br. 108, naročito što se tiče uslova koji se odnosi na identifikovane osobe ili osobe koje je moguće identifikovati[153].

OUZP-om se utvrđuje da se pojedincu identitet može utvrditi kada se on „može identifikovati direktno ili indirektno, naročito uz pomoć identifikatora kao što su ime, identifikacioni broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više činilaca svojstvenih fizičkom, fiziološkom, genetskom, mentalnom, ekonomskom, kulturnom ili socijalnom identitetu tog pojedinca"[154]. Identifikacija zato podrazumeva elemente koji osobu opisuju tako da se razlikuje od svih drugih osoba i prepoznaje kao pojedinac. Ime osobe je prvi primer takvih elemenata opisa i omogućava direktnu identifikaciju osobe. U nekim slučajevima drugi atributi mogu imati sličan učinak kao ime i omogućiti indirektnu identifikaciju osobe. Telefonski broj, broj socijalnog osiguranja i registracioni broj vozila primeri su informacija prema kojima je pojedinca moguće identifikovati. Atributi kao što su računarske datoteke, „kolačići" i alati za nadzor mrežnog saobraćaja mogu da se upotrebe i za selekciju/izdvajanje pojedinaca identifikovanjem njihovog ponašanja i navika. Kako je objašnjeno u mišljenju Radne grupe iz člana 29. „[č]ak i bez upita o imenu i adresi pojedinca moguće ga je kategorisati na osnovu socioekonomskih, psiholoških, filozofskih i drugih kriterijuma ili pripisati mu određene odluke budući da za kontakt tačku (računar) pojedinca više nije potrebno otkrivanje njegovog identiteta u užem smislu"[155]. Definicija ličnih podataka i prema pravu Saveta Evrope i pravu EU dovoljno je široka da obuhvata sve mogućnosti identifikacije (i stoga i sve stepene identifikacije).

152 Opšta uredba o zaštiti podataka, uvodna izjava 26.

153 Videti ESLJP, *Amann protiv Švajcarske* [VV], br. 27798/95, 16. februara 2000., stav 65.

154 Opšta uredba o zaštiti podataka, član 4. stav 1.

155 Radna grupa iz člana 29., *Opinion 4/2007 on the concept of personal data* (Mišljenje 4/2007 o konceptu ličnih podataka), WP 136, 20. juna 2007., str. 15.

Primer: U predmetu *Promusicae protiv Telefónica de España*[156] SPEU je izjavio da „je nesporno da dostavljanje imena i adresa pojedinih korisnika [određene internet platforme za zajedničko korišćenje datoteka] koje je zatražila organizacija Promusicae uključuje stavljanje na raspolaganje ličnih podataka, odnosno informacija koje se tiču identifikovanih fizičkih lica ili fizičkih lica koje je moguće identifikovati, u skladu sa definicijom iz člana 2. tačka (a) Direktive 95/46 [trenutno član4. stav 1. OUZP-a]. Takvo dostavljanje informacija koje je, kako je iznela Promusicae, a Telefónica nije osporila, Telefónica sačuvala, predstavlja obradu ličnih podataka"[157].

Primer: Predmet *Scarlet Extended SA protiv Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*[158] odnosio se na odbijanje pružaoca usluga interneta Scarlet da instalira sistem za filtriranje elektronskih komunikacija, koje se služe softverom za zajedničko korišćenje datotekama, kako bi se sprečilo zajedničko korišćenje datotekama kojim se krše autorska prava koja štiti SABAM, upravljačko društvo koje zastupa autore, kompozitore i urednike. SPEU je utvrdio da su IP adrese „zaštićeni lični podaci jer omogućavaju identifikaciju korisnika".

Budući da mnoga imena nisu jedinstvena, za utvrđivanje identiteta osobe mogu biti potrebni dodatni atributi kako bi se obezbedilo da se osoba ne zameni sa nekom drugom. Ponekad se direktni i indirektni atributi moraju kombinovati kako bi se identifikovao pojedinac na koga se informacije odnose. Često se upotrebljavaju datum i mesto rođenja. U pojedinim zemljama su takođe uvedeni personalizovani brojevi kako bi se građani bolje međusobno razlikovali. Preneseni poreski podaci[159], podaci koji se odnose na podnosioca zahteva za dozvolu boravka sadržani u administrativnom dokumentu[160] i dokumenti koji se odnose na bankarske i fiducijarne odnose[161] mogu da predstavljaju lične podatke. Biometrijski podaci, kao što su otisci prstiju,

156 SPEU, C-275/06, *Productores de Música de España (Promusicae) protiv Telefónica de España SAU* [VV], 29. januara 2008., stav 45.

157 Nekadašnja Direktiva 95/46/EZ, član 2. tačka (b), sada Opšta uredba o zaštiti podataka, član 4. stav 2.

158 SPEU, C-70/10, *Scarlet Extended SA protiv Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. novembra 2011, stav 51.

159 SPEU, C-201/14, *Smaranda Bara i dr. protiv Casa Națională de Asigurări de Sănătate i dr.*, 1. oktobra 2015.

160 SPEU, *Y. S. protiv Minister voor Immigratie, Integratie en Asiel i Minister voor Immigratie, Integratie en Asiel protiv M. i S.*, 17. jula 2014.

161 ESLJP, *M. N. i drugi protiv San Marina*, br. 28005/12, 7. jula 2015.

digitalne fotografije ili skeniranja zenice oka, podaci o lokaciji i mrežni atributi sve su važniji za identifikovanje osoba u tehnološko doba.

Međutim, preduslov za primenjivost evropskog prava zaštite podataka nije stvarna identifikacija ispitanika. Dovoljno je da dotična osoba može da se identifikuje. Smatra se da se osoba može identifikovati ako je dostupno dovoljno elemenata na osnovu kojih se osoba može direktno ili indirektno identifikovati[162]. U skladu sa uvodnom izjavom 26 OUZP-a, to se procenjuje na osnovu verovatnoće da će predvidivim korisnicima informacija biti dostupni prihvatljivi instrumenti identifikacije i da će ih korisnici primeniti, što uključuje informacije koje imaju primaoci treće strane (videti deo 2.3.2).

Primer: Lokalno telo odluči da prikuplja podatke o vozilima koja prebrzo voze lokalnim putevima. Potom fotografiše vozila, istovremeno snimajući vreme i lokaciju, kako bi te podatke prosledilo nadležnom organu radi kažnjavanja prestupnika. Ispitanik ulaže žalbu tvrdeći da lokalni organ, u skladu sa zakonodavstvom o zaštiti podataka, nema pravne osnove za takvo prikupljanje podataka. Lokalni organ smatra da ne prikuplja lične podatke, tvrdeći da su podaci o registraciji anonimni. Lokalni organ nema pravno ovlašćenje pristupa opštem registru vozila za otkrivanje identiteta vlasnika vozila ili vozača.

Taj argument se ne podudara sa uvodnom izjavom 26 OUZP-a. S obzirom na to da je očigledna svrha prikupljanja podataka identifikovati i kazniti prekršioce, u izgledu je da će se pokušati izvršenje identifikacije. Premda lokalni organi nemaju direktan pristup sredstvima identifikacije, oni će podatke proslediti nadležnom organu, odnosno policiji, koja raspolaže tim sredstvima. Iz uvodne izjave 26 takođe jasno proizlazi scenario prema kojem se može predvideti da dalji primaoci podataka, osim neposrednog korisnika podataka, mogu pokušati da identifikuju pojedinca. U kontekstu uvodne izjave 26, radnja koju je preduzeo lokalni organ izjednačena je sa prikupljanjem podataka o osobama koje se mogu identifikovati pa je stoga za nju, u skladu sa pravom zaštite podataka, potrebna pravna osnova.

„Kako bi se utvrdilo da li je po svemu sudeći u izgledu da se upotrebljavaju sredstva za utvrđivanje identiteta pojedinca, trebalo bi uzeti u obzir sve objektivne činioce,

162 Opšta uredba o zaštiti podataka, član 4. stav 1.

kao što su troškovi i vreme potrebno za utvrđivanje identiteta, uzimajući u obzir i tehnologiju dostupnu u vreme obrade i tehnološki razvoj"[163].

Primer: U predmetu *Breyer protiv Bundesrepublik Deutschland*[164] SPEU je razmatrao koncept moguće indirektne identifikacije ispitanika. Predmet se odnosio na dinamičke IP adrese, koje se menjaju svaki put kada se uspostavi nova veza s internetom. Internet strane kojima upravljaju nemačke savezne institucije registrovale su i pohranjivale dinamičke IP adrese kako bi se sprečili sajber napadi i po potrebi pokrenuli krivični postupci. Samo je pružalac usluga interneta, kojim se služio g. Breyer, imao dodatne informacije potrebne za njegovu identifikaciju.

SPEU je smatrao da dinamička IP adresa, koju pružalac usluga elektronskih medija registruje kada korisnik pristupi internet stranici koju je pružalac stavio na raspolaganje javnosti, predstavlja lični podatak samo ako treća strana, odnosno pružalac usluga interneta u ovom slučaju, ima dodatne podatke potrebne za identifikaciju te osobe[165]. SPEU je istakao da „nije potrebno da sve informacije koje omogućavaju identifikaciju osobe o kojoj je reč moraju da se nalaze u posedu samo jedne osobe" da bi informacije mogle da se kvalifikuju kao lični podaci. Korisnici dinamičkih IP adresa koje registruje pružalac usluga interneta mogu se identifikovati u određenim situacijama, na primer u okviru krivičnog postupka u slučaju sajber napada, uz pomoć drugih osoba[166]. Prema SPEU, ako pružalac usluga „raspolaže pravnim sredstvima koja mu omogućavaju identifikaciju navedene osobe pomoću dodatnih informacija kojima raspolaže pružalac pristupa internetu te osobe", to predstavlja „sredstvo koje se može opravdano koristiti za utvrđivanje navedene osobe". Stoga se takvi podaci smatraju ličnim podacima.

Na osnovu prava Saveta Evrope, mogućnost identifikacije tumači se na sličan način. Izveštaj sa objašnjenjima o modernizovanoj Konvenciji br. 108 sadrži sličan opis: koncept „mogućnosti identifikacije" ne odnosi se samo na građanski ili pravni iden-

163 *Ibid*., uvodna izjava 26.

164 SPEU, C-582/14, *Patrick Breyer protiv Bundesrepublik Deutschland*, 19. oktobra 2016, stav 43.

165 Nekadašnja Direktiva 95/46/EZ Evropskog parlamenta i Saveta od 24. oktobra 1995. o zaštiti pojedinaca u vezi sa obradom ličnih podataka i o slobodnom protoku takvih podataka, član 2. tačka (a).

166 SPEU, C-70/10, *Scarlet Extended SA protiv Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. novembra 2011, st. 47 i 48.

titet pojedinca, nego i na sve što može omogućiti „individualizaciju" odnosno izdvajanje pojedinca u odnosu na druge, a stoga i moguće drugačije postupanje prema njemu. Ta „individualizacija" se može izvesti, na primer, posebnim upućivanjem na tu osobu ili na uređaj ili kombinaciju uređaja (računar, mobilni telefon, kamera, konzole za igrice itd.) koji su povezani sa identifikacionim brojem, pseudonimom, biometrijskim ili genetskim podacima, podacima o lokaciji, IP adresom ili drugim identifikatorom[167]. Ne smatra se da se pojedinac „može identifikovati" ako je za njegovu identifikaciju potrebno neuobičajeno mnogo vremena, truda i resursa. To je slučaj, na primer, kada bi za identifikaciju ispitanika bile potrebne prekomerno složene, duge i skupocene radnje. Nerazumnost utrošenog vremena, truda i resursa mora se proceniti u svakom pojedinačnom slučaju, uzimajući u obzir činioce kao što su svrha obrade, cene i koristi identifikacije, vrste rukovalaca podacima i primenjene tehnologije[168].

Važno je napomenuti da oblik u kojem se lični podaci čuvaju ili upotrebljavaju nije relevantan za primenjivost propisa o zaštiti podataka. Pismena ili usmena komunikacija može sadržati lične podatke kao i slike[169], uključujući snimak[170] ili zvuk[171] televizije zatvorenog kruga (CCTV). Elektronski snimljene informacije, kao i informacije na papiru, takođe mogu biti lični podaci. Čak i uzorci ćelija ljudskog tkiva, u kojima se beleži DNK pojedinca, mogu biti izvori iz kojih se mogu izdvojiti biometrijski podaci[172] ako se ti podaci odnose na nasleđena ili stečena genetska obeležja pojedinca, ako daju jedinstvene informacije o njegovom zdravlju ili fiziologiji i ako proizlaze iz analize biološkog uzorka te osobe[173].

---

167 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 18.

168 *Ibid*., t. 17.

169 ESLJP, *Von Hannover protiv Nemačke*, br. 59320/00, 24. juna 2004; ESLJP, *Sciacca protiv Italije*, br. 50774/99, 11. januara 2005; SEU, C-212/13, *František Ryneš protiv Úřad pro ochranu osobních údajů,* 11. decembra 2014.

170 ESLJP, *Peck protiv Ujedinjenog Kraljevstva*, br. 44647/98, 28. januara 2003; ESLJP, *Köpke protiv Nemačke* (odl.), br. 420/07, 5. oktobra 2010; EDPS (2010), *The EDPS video-surveillance guidelines* (Smernice EDPS-a o video-nadzoru), 17. marta 2010.

171 ESLJP, *P. G. i J. H. protiv Ujedinjenog Kraljevstva*, br. 44787/98, 25. septembra 2001, t. 59 i 60; ESLJP, *Wisse protiv Francuske*, br. 71611/01, 20. decembra 2005. (verzija na francuskom jeziku).

172 Vidi Radna grupa iz člana 29. (2007), *Opinion 4/2007 on the concept of personal data* (Mišljenje 4/2007 o konceptu ličnih podataka), WP136, 20. juna 2007, str. 9; Savet Evrope, Recommendation No. Rec(2006)4 of the Committee of Ministers to member states on research on biological materials of human origin (Preporuka br. Rec(2006)4 Saveta ministara državama članicama o istraživanju bioloških materijala ljudskog porekla), 15. marta 2006.

173 Opšta uredba o zaštiti podataka, član 4. stav 13.

Anonimizacija/Izostavljanje

U skladu sa načelom ograničenog čuvanja podataka sadržanom u Opštoj uredbi o zaštiti podataka, kao i modernizovanoj Konvenciji br. 108 (o kojem se detaljnije raspravlja u poglavlju 3), podaci se moraju čuvati „u obliku koji omogućava identifikaciju ispitanikâ samo onoliko dugo koliko je potrebno u svrhe radi kojih se lični podaci obrađuju"[174]. U skladu sa tim, kada podaci više nisu potrebni i ne služe prvobitnoj svrsi, moraju se izbrisati ili anonimizovati/izostaviti ako rukovalac podacima želi da ih sačuva.

Postupak anonimizacije/izostavljanja podataka podrazumeva da su svi elementi identifikacije uklonjeni iz grupe ličnih podataka kako ispitanik više ne bi mogao da se identifikuje[175]. Radna grupa iz člana 29. u svom Mišljenju 05/2014 analizira delotvornost i ograničenja različitih tehnika anonimizacije/izostavljanja[176]. Ona potvrđuje moguću vrednost takvih tehnika, ali naglašava da određene tehnike nisu nužno primenjive u svim slučajevima. Da bi se pronašlo optimalno rešenje u određenoj situaciji, odgovarajući postupak anonimizacije/izostavljanja treba da se odredi za svaki pojedinačni slučaj. Nezavisno od tehnike koja se primenjuje, identifikacija se mora sprečiti, i to nepovratno. To znači da, kako bi podaci bili anonimizovani, ne sme da bude prisutan nijedan elemenat u informacijama koji bi uz ulaganje razumnog truda mogao da posluži za ponovnu identifikaciju dotične osobe (ili osoba)[177]. Rizik od ponovne identifikacije može se proceniti uzimajući u obzir „vreme, trud ili resurse potrebne s obzirom na prirodu podataka, kontekst njihove upotrebe, dostupne tehnologije za ponovnu identifikaciju i povezane troškove"[178].

Kada su podaci uspešno anonimizovani/izostavljeni, više nisu lični i zakonodavstvo o zaštiti podataka više se ne primenjuje.

OUZP-om se propisuje da se osoba ili organizacija koja nadgleda obradu ličnih podataka ne može obavezati na čuvanje, prikupljanje ili obradu dodatnih podataka za identifikaciju ispitanika isključivo radi usklađivanja sa Uredbom. Međutim, to pra-

174 *Ibid*., član 5. stav 1. tačka (e); modernizovana Konvencija br. 108, član 5. stav 4. tačka (e).

175 Opšta uredba o zaštiti podataka, uvodna izjava 26.

176 Radna grupa iz člana 29 (2014), *Opinion 05/2014 on Anonymization Techniques* (Mišljenje 05/2014 o tehnikama anonimizacije), WP 216, 10. aprila 2014.

177 Opšta uredba o zaštiti podataka, uvodna izjava 26.

178 Savet Evrope, Odbor za Konvenciju br. 108 (2017), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data* (Smernice o zaštiti pojedinaca u pogledu obrade ličnih podataka u svetu velikih podataka), 23. januara 2017, t. 6.2.

vilo ima značajan izuzetak: kad god ispitanik pruži dodatne informacije rukovaocu podacima koje omogućavaju njegovu identifikaciju, radi ostvarivanja prava na pristup ličnim podacima, ispravka ili brisanje podataka, ograničavanje obrade i prenosivost podataka, tada podaci koji su prethodno anonimizovani ponovo postaju lični podaci[179].

Pseudonimizacija/Zamena

Lični podaci sadrže atribute poput imena, datuma rođenja, pola i adrese ili druge elemente koji mogu da dovedu do identifikacije. Postupak pseudonimizacije/zamene ličnih podataka podrazumeva zamenu tih atributa pseudonimom.

U **pravu EU** „pseudonimizacija" se definiše kao „obrada ličnih podataka na način da se lični podaci više ne mogu pripisati određenom ispitaniku bez upotrebe dodatnih informacija, pod uslovom da se takve dodatne informacije drže odvojeno i da podležu tehničkim i organizacionim merama kako bi se obezbedilo da lični podaci ne mogu da se pripišu pojedincu čiji je identitet utvrđen ili može da se utvrdi"[180]. Za razliku od anonimizovanih podataka, pseudonimizovani podaci i dalje su lični podaci i zato podležu zakonodavstvu o zaštiti podataka. Iako se pseudonimizacijom mogu smanjiti bezbednosni rizici za ispitanike, ona nije izuzeta iz područja primene OUZP-a.

U OUZP-u su prepoznate različiti načini primene pseudonimizacije kao primerene tehničke mere za poboljšanje zaštite podataka, a posebno se navodi za oblik i bezbednost obrade podataka[181]. To je takođe primerena zaštitna mera koja se može upotrebiti za obradu ličnih podataka u svrhe za koje nisu prvobitno prikupljeni[182].

Pseudonimizacija/zamena se ne spominje izričito u pravnim definicijama modernizovane Konvencije br. 108 **Saveta Evrope**. Međutim, u Izveštaju s objašnjenjima o modernizovanoj Konvenciji br. 108 jasno se navodi da „upotreba pseudonima ili bilo kog digitalnog identifikatora/digitalnog identiteta ne dovodi do anonimizacije podataka jer se ispitanik i dalje može identifikovati ili individualizovati"[183]. Jedan od načina na koji se podaci mogu pseudonimizovati jeste šifrovanje podataka. Nakon pseudonimizacije podataka, veza s identitetom postoji u obliku pseudonima uz ključ

179 Opšta uredba o zaštiti podataka, član 11.

180 *Ibid*., član 4. stav 5.

181 *Ibid*., član 25. stav 1.

182 *Ibid*., član 6. stav 4.

183 Izveštaj sa objašnjenjima o modernizovanoj Konvenciji br. 108, stav 18.

za dešifrovanje. Bez tog ključa teško je identifikovati pseudonimizovane podatke. Međutim, oni koji su ovlašćeni da upotrebljavaju takav ključ mogu ponovo na jednostavan način da identifikuju osobu. Posebno treba sprečiti da neovlašćene osobe upotrebljavaju ključeve za dešifrovanje. Stoga se „[p]seudonimni podaci [...] smatraju ličnim podacima [...]" obuhvaćenim modernizovanom Konvencijom br. 108[184].

Autentifikacija/Potvrđivanje

Autentifikacija je postupak u kojem osoba može da dokaže da ima određeni identitet i/ili da je ovlašćena za određene radnje, kao što je pristup bezbednosnim zonama ili podizanje novca sa bankovnog računa. Autentifikacija/Potvrđivanje se može izvršiti poređenjem biometrijskih podataka, kao što je fotografija ili otisak prsta u pasošu, s podacima kojima se osoba predstavlja prilikom, na primer, imigracione kontrole[185]; ili traženjem podataka koje bi trebalo da zna samo osoba određenog identiteta ili s određenim ovlašćenjem, kao što je jedinstveni identifikacioni broj (PIN) ili lozinka; ili traženjem na uvid određenog tokena koji bi trebalo da bude u isključivom posedu osobe određenog identiteta ili sa određenim ovlašćenjem, kao što su posebna čip-kartica ili ključ bankovnog sefa. Osim lozinki ili čip-kartica, elektronski potpis, ponekad zajedno sa PIN-ovima, predstavlja vrlo delotvorno sredstvo identifikacije i potvrđivanja osobe u elektronskim komunikacijama.

2.1.2. Posebne kategorije ličnih podataka

Na osnovu prava EU kao i **prava Saveta Evrope** postoje posebne kategorije ličnih podataka koji zbog svoje prirode prilikom obrade mogu da predstavljaju rizik za ispitanike, pa ih zato treba dodatno zaštititi. Takvi podaci podležu principu zabrane i uslovi u kojima je takva obrada zakonita jesu ograničeni.

U okviru modernizovane Konvencije br. 108 (član 6.) i OUZP-a (član 9.), sledeće kategorije se smatraju osetljivim podacima:

- lični podaci kojima se otkriva rasno ili etničko poreklo,
- lični podaci kojima se otkrivaju politička mišljenja, verska ili druga uverenja, uključujući filozofske stavove,

184 *Ibid.*

185 *Ibid.*, st. 56 i 57.

- lični podaci kojima se otkriva članstvo u sindikatima,
- genetski i biometrijski podaci koji se obrađuju u svrhu identifikacije osobe,
- lični podaci u vezi sa zdravljem, polnim životom ili seksualnom orijentacijom.

Primer: Predmet *Bodil Lindqvist*[186] odnosio se na upućivanje na različite osobe na internet stranici navođenjem njihovog imena ili na druge načine, na primer, navođenjem njihovog telefonskog broja ili informacija o njihovim hobijima. SPEU je izjavio da „pozivanje na činjenicu da je osoba povredila stopalo, a zaposlena je na nepuno radno vreme iz medicinskih razloga predstavlja lične podatke koji se tiču zdravlja"[187].

Lični podaci povezani s krivičnim delima i osudama

U modernizovanoj Konvenciji br. 108 navode se lični podaci koji se odnose na krivična dela, krivične postupke i osude, kao i s njima povezane bezbednosne mere u sklopu popisa posebnih kategorija ličnih podataka[188]. U okviru OUZP-a lični podaci koji se odnose na krivična dela, krivične postupke i osude, kao i s njima povezane bezbednosne mere, ne spominju se u sklopu popisa posebnih kategorija podataka, ali se obrađuju u zasebnom članu. U članu 10. OUZP-a utvrđuje se da se obrada takvih podataka može vršiti samo „pod nadzorom službenog tela ili kada je obrada odobrena pravom Unije ili pravom države članice kojim se propisuju odgovarajuće zaštitne mere za prava i slobode ispitanikâ". S druge strane, sveobuhvatni registri podataka o krivičnim osudama mogu da se vode pod nadzorom određenih službenih tela[189]. Obrada ličnih podataka u kontekstu sprovođenja prava u EU se reguliše posebnim pravnim instrumentom, Direktivom 2016/680/EU[190]. Direktivom se utvrđuju posebna pravila zaštite podataka, koja su obavezujuća za nadležna tela kada obrađuju lične podatke u svrhu sprečavanja, istrage, otkrivanja i gonjenja krivičnih dela (videti deo 8.2.1).

186 SPEU, C-101/01, *Krivični postupak protiv Bodil Lindqvist*, 6. novembra 2003, stav 51.

187 Nekadašnja Direktiva 95/46/EZ, član 8. tačka (1), sada Opšta uredba o zaštiti podataka, član 9. stav 1.

188 Modernizovana Konvencija br. 108, član 6. stav 1.

189 Opšta uredba o zaštiti podataka, član 10.

190 Direktiva (EU) 2016/680 Evropskog parlamenta i Saveta od 27. aprila 2016. o zaštiti pojedinaca u vezi sa obradom ličnih podataka od strane nadležnih tela u svrhe sprečavanja, istrage, otkrivanja ili gonjenja krivičnih dela ili izvršavanja krivičnih sankcija i o slobodnom kretanju takvih podataka kao i o stavljanju van snage Okvirne odluke Saveta 2008/977/PUP, SL 2016 L 119.

2.2. Obrada podataka

Ključne tačke

- „Obrada podataka" odnosi se na svaku radnju koja se vrši nad ličnim podacima.
- Pojam „obrada" obuhvata automatizovanu i neautomatizovanu obradu.
- Prema pravu EU „obrada" se odnosi i na ručnu obradu u strukturisanim sistemima arhiviranja.
- Prema pravu Saveta Evrope značenje „obrade" može se proširiti u okviru domaćeg zakonodavstva kako bi obuhvatilo ručnu obradu.

2.2.1. Koncept obrade podataka

Koncept obrade ličnih podataka sveobuhvatno je definisan **i u pravu EU i pravu Saveta Evrope**: „‚obrada ličnih podataka' [...] znači svaki postupak [...] kao što su prikupljanje, beleženje, organizacija, strukturisanje, čuvanje, prilagođavanje ili izmena, pronalaženje, obavljanje uvida, upotreba, otkrivanje prenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombinovanje, ograničavanje, brisanje ili uništavanje"[191] ličnih podataka. U modernizovanoj Konvenciji br. 108 definiciji se dodaje čuvanje ličnih podataka[192].

Primer: U predmetu *František Ryneš*[193] g. Rineš snimio je fotografiju dveju osoba koje su razbile prozore na njegovom domu, pomoću kućnog sistema video-nadzora sa televizijom zatvorenog kruga (CCTV) koji je postavio radi zaštite svoje imovine. SPEU je utvrdio da video-nadzor koji uključuje snimanje i čuvanje ličnih podataka predstavlja automatsku obradu podataka koja je obuhvaćena oblašću primene zakonodavstva EU o zaštiti podataka.

191 Opšta uredba o zaštiti podataka, član 4. stav 2. Videti i modernizovanu Konvenciju br. 108, član 2. tačka (b).

192 Modernizovana Konvencija br. 108, član 2. tačka (b).

193 SPEU, C-212/13, *František Ryneš protiv Úřad pro ochranu osobních údajů*, 11. decembra 2014, stav 25.

Primer: U predmetu *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce protiv Salvatorea Mannija*[194] g. Mani zatražio je uklanjanje svojih ličnih podataka iz registra za rejting trgovačkih kompanija koji su ga povezivali sa likvidacijom kompanije za poslovanje nekretninama i tako negativno uticali na njegov ugled. SPEU je smatrao da „upisivanjem i čuvanjem navedenih podataka u registru i njihovom dostavom, prema potrebi, na zahtev trećih lica, telo zaduženo za vođenje tog registra vrši 'obradu ličnih podataka' za koju je 'odgovorno'".

Primer: Poslodavci prikupljaju i obrađuju podatke o svojim zaposlenima, uključujući informacije o njihovim platama. Pravna osnova za zakonitost tog čina jeste ugovor o radu.

Poslodavci podatke o platama zaposlenih prosleđuju poreskim organima. Takvo prosleđivanje podataka se takođe smatra „obradom" u smislu značenja tog pojma u modernizovanoj Konvenciji br. 108 i OUZP-u. Međutim, pravna osnova za takvo otkrivanje podataka nije ugovor o radu. Mora postojati dodatna pravna osnova za postupke obrade koji podrazumevaju prenos podataka o platama od poslodavca do poreskog organa. Ta pravna osnova je obično sadržana u odredbama domaćih poreskih zakona. Bez takvih odredbi, i bez neke druge legitimne osnove za obradu, takav prenos podataka smatrao bi se nezakonitom obradom.

2.2.2. Automatizovana obrada podataka

Zaštita podataka na osnovu modernizovane Konvencije br. 108 i OUZP-a u potpunosti se primenjuje na automatizovanu obradu podataka.

Na osnovu **prava EU**, automatizovana obrada podataka odnosi se na radnje izvršene na ličnim podacima delimično ili u celini automatizovanim sredstvima[195]. Modernizovana Konvencija br. 108 sadrži sličnu definiciju[196]. U praktičnom smislu, to znači da

194 SPEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce protiv Salvatorea Mannija*, 9. marta 2017., stav 35.

195 Opšta uredba o zaštiti podataka, član 2. stav 1. i član 4. stav 2.

196 Modernizovana Konvencija br. 108, član 2. tačke (b) i (c); Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 21.

je svaka obrada ličnih podataka automatizovanim sredstvima pomoću, na primer, ličnog računara, mobilnog uređaja ili rutera, obuhvaćena propisima o zaštiti podataka EU i Saveta Evrope.

Primer: Predmet *Bodil Lindqvist*[197] odnosio se na upućivanje na različite osobe na internet stranici navođenjem njihovo imena ili na druge načine, na primer, navođenjem njihovog telefonskog broja ili informacija o njihovim hobijima. SPEU je zaključio da „navođenje različitih osoba na internet stranici i njihovo identifikovanje putem imena i prezimena ili na drugi način, na primer navođenjem njihovog telefonskog broja ili informacija u vezi s njihovim radnim uslovima ili hobijima, predstavlja, podatke koji se u celosti ili delimično obrađuju automatskim putem" u smislu člana 3. stav 1. Direktive 95/46/EZ[198].

Primer: U predmetu *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González*[199] g. Gonzalez zatražio je uklanjanje ili izmenu linka između njegovog imena u internet pretraživaču Gugl i dveju strana u novinama u kojima je objavljena licitacija nekretnina radi naplate dugovanja za socijalno osiguranje. SPEU je naveo da „pretražujući internet na automatizovan, stalan i sistematičan način u potrazi za informacijama koje su na njemu objavljene, operater pretraživača ‚prikuplja' takve podatke koje zatim ‚vraća', ‚snima' i ‚organizuje' u okviru svojih programa indeksiranja, ‚čuva' na svojim serverima i u određenim slučajevima ‚otkriva' i ‚stavlja na raspolaganje' svojim korisnicima rezultate njihovih pretraga u obliku popisa"[200]. SPEU je zaključio da takve radnje predstavljaju „obradu", „bez obzira na to što operater pretraživača iste operacije podjednako primenjuje na druge vrste informacija i što ne razlikuje njih i lične podatke".

197 SPEU, C-101/01, *Krivični postupak protiv Bodil Lindqvist*, 6. novembra 2003, stav 27.

198 Opšta uredba o zaštiti podataka, član 2. stav 1.

199 SPEU, C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González* [VV], 13. maja 2014.

200 Ibid., stav 28

2.2.3. Neautomatizovana obrada podataka

Ručna obrada podataka takođe zahteva zaštitu podataka.

Zaštita podataka **na osnovu prava EU** ni na koji način nije ograničena na automatizovanu obradu podataka. U skladu s tim, na osnovu prava EU zaštita podataka primenjuje se na obradu ličnih podataka u ručnom sistemu arhiviranja, tj. posebno strukturiranoj papirnoj datoteci[201]. Strukturirani sistem arhiviranja je sistem u kome se kategoriše skup ličnih podataka tako da su oni dostupni na osnovu određenih merila. Na primer, ako poslodavac vodi papirnu datoteku pod nazivom „slobodni dani zaposlenih", u kojoj su sadržane sve pojedinosti o slobodnim danima koje je osoblje uzelo u protekloj godini i koja je organizovana po azbučnom redu, datoteka će činiti ručni sistem arhiviranja koji podleže propisima EU o zaštiti podataka. Razlog takvog proširenja zaštite podataka jeste to što:

- papirne datoteke mogu da se strukturiraju tako da omogućavaju brzo i jednostavno pronalaženje informacija,

- čuvanjem ličnih podataka u strukturiranim papirnim datotekama lakše zaobilaze zakonski propisana ograničenja automatizovane obrade podataka[202].

Na osnovu **prava Saveta Evrope**, u definiciji automatske obrade prepoznato je da među pojedinim automatizovanim radnjama mogu biti potrebne određene faze ručne upotrebe ličnih podataka[203]. Članom 2 tačka (c) modernizovane Konvencije br. 108 utvrđuje se da „[a]ko se ne upotrebljava automatizovana obrada, obrada podataka podrazumeva radnju ili skup radnji izvršenih na ličnim podacima unutar strukturiranog skupa takvih podataka koji je dostupan ili se može pronaći u skladu sa određenim kriterijumima".

201 Opšta uredba o zaštiti podataka, član 2. stav 1.

202 Opšta uredba o zaštiti podataka, uvodna izjava 15.

203 Modernizovana Konvencija br. 108, član 2. tačke (b) i (c).

2.3. Korisnici ličnih podataka

Ključne tačke

- Osoba koja odlučuje o načinima i svrhama obrade ličnih podataka drugih naziva se „rukovalac podacima" u skladu sa pravom zaštite podataka. Ako nekoliko osoba zajednički donosi tu odluku, one mogu biti „zajednički rukovaoci podacima".
- „Obrađivač podataka" je fizičko ili pravno lice koje obrađuje lične podatke u ime rukovaoca podacima.
- Obrađivač podataka postaje rukovalac podacima ako odlučuje o načinima i svrhama same obrade podataka.
- Svaka osoba kojoj se prenesu podaci je „primalac".
- „Treća strana" je fizičko ili pravno lice koje nije ispitanik, rukovalac podacima, obrađivač podataka ni osoba koja je ovlašćena za obradu ličnih podataka pod neposrednom nadležnošću rukovaoca podacima ili obrađivača podataka.
- Odobrenje/saglasnost kao pravna osnova za obradu ličnih podataka mora biti dobrovoljno dato, utemeljeno na informacijama, poseban i nedvosmislen znak želje potvrđen jasnim činom koji predstavlja pristajanje na obradu.
- Za obradu posebnih kategorija podataka na osnovu odobrenja potrebno je izričito odobrenje.

2.3.1. Rukovalac podacima i obrađivač podataka

Najvažnija posledica obavljanja funkcije rukovoca podacima ili obrađivača podataka jeste pravna odgovornost za ispunjavanje odgovarajućih obaveza koje proizlaze iz prava zaštite podataka. U privatnom sektoru je to obično fizičko ili pravno lice, a u javnom sektoru nadležni organ. Postoji značajna razlika između rukovaoca podacima i obrađivača podataka: rukovalac podacima je fizičko ili pravno lice koje donosi odluke o svrhama i načinima obrade, a obrađivač podataka je fizičko ili pravno lice koje obrađuje podatke u ime rukovaoca podacima, pridržavajući se strogih uputstava. U načelu, rukovalac podacima vrši nadzor nad obradom i snosi odgovornost za nju, uključujući pravnu odgovornost. Međutim, od uvođenja reformi propisa o zaštiti podataka, obrađivači podataka imaju obavezu usklađivanja s mnoštvom zahteva koji se primenjuju na rukovaoce podacima. Na primer, prema OUZP-u obrađivači podataka moraju da vode evidenciju svih kategorija aktivnosti obrade kako bi dokazali

usklađenost sa obavezama koje imaju na osnovu Uredbe[204]. Obrađivači podataka takođe moraju da sprovedu odgovarajuće tehničke i organizacione mere kako bi osigurali bezbednost obrade[205], imenuju službenika za zaštitu podataka u određenim slučajevima[206] i obaveste rukovaoca podacima o povredama podataka[207].

Da li će osoba moći da odredi i utvrdi svrhu i načine obrade zavisiće od činjenica ili okolnosti pojedinačnog slučaja. Prema definiciji rukovaoca podacima iz OUZP-a, tu funkciju mogu vršiti fizička lica, pravna lica ili bilo koja druga tela. Međutim, Radna grupa iz člana 29. naglasila je da bi se za davanje pojedincima stabilnijeg subjekta putem kojeg mogu ostvariti svoja prava „za funkciju rukovaoca podacima trebalo razmatrati kompaniju ili telo kao takvo, umesto određene osobe unutar kompanije ili tela"[208]. Na primer, kompanija koje prodaje medicinske potrepštine lekarima je rukovalac podacima za sastavljanje i vođenje popisa za distribuciju koji sadrži sve lekare na određenom području, a ne menadžer prodaje koji zaista upotrebljava i vodi popis.

Primer: Kad marketinški sektor kompanije Sunshine planira da obrađuje podatke u svrhe istraživanja tržišta, onda je rukovalac podacima kompanija Sunshine, a ne zaposleni marketinškog sektora. Marketinški sektor ne može biti rukovalac podacima jer nema zasebno pravno lice.

Fizička lica mogu biti rukovaoci podacima i prema pravu Unije i Saveta Evrope. Međutim, prilikom obrade podataka o drugim licima koji se odnose na isključivo ličnu ili kućnu aktivnost, pojedinci ne potpadaju pod pravila iz OUZP-a i modernizovane Konvencije br. 108, pa se ne smatraju rukovaocima podacima[209]. Pojedinac koji čuva zapise o svojoj prepisci, vodi lični dnevnik u kome opisuje događaje koji uključuju prijatelje i saradnike, kao i evidenciju o zdravstvenom stanju članova porodice, može biti izuzet od propisa o zaštiti podataka jer te aktivnosti mogu biti isključivo lične ili kućne. U OUZP-u se dodatno utvrđuje da lične ili kućne aktivnosti takođe

204 Opšta uredba o zaštiti podataka, član 30. stav 2.

205 *Ibid*., član 32.

206 *Ibid*., član 37.

207 *Ibid*., član 33. stav 2.

208 Radna grupa iz člana 29. (2010), *Opinion 1/2010 on the concepts of „controller" and „processor"* (Mišljenje 1/2010 o pojmovima „rukovalac podacima" i „obrađivač podataka"), WP 169, Bruxelles, 16. februara 2010.

209 Opšta uredba o zaštiti podataka, uvodna izjava 18 i član 2. stav 2. tačka (c); modernizovana Konvencija br. 108, član 3. tačka (2).

mogu uključivati socijalno umrežavanje i internet aktivnosti preduzete u kontekstu takvih aktivnosti[210]. S druge strane, propisi o zaštiti podataka u potpunosti se primenjuju na rukovaoce podacima i obrađivače podataka koji daju sredstva za obradu ličnih podataka za lične ili kućne aktivnosti (na primer, platforme društvenih mreža)[211].

Pristup građana internetu i njihova mogućnost upotrebe platformi za e-trgovinu, društvenih mreža i internet stranica s blogovima za deljenje ličnih podataka o sebi i drugim osobama sve više otežavaju razdvajanje lične od nelične obrade[212]. Da li su aktivnosti isključivo lične ili kućne zavisi od okolnosti[213]. Aktivnosti koje imaju profesionalne ili komercijalne aspekte ne mogu da budu izuzete kao kućne aktivnosti[214]. Stoga kada opseg i učestalost obrade podataka ukazuju na profesionalnu aktivnost ili aktivnost na puno radno vreme, pojedinac se može smatrati rukovaocem podacima. Uz profesionalna ili komercijalna obeležja aktivnosti obrade, dodatni faktor koji se mora uzeti u obzir jeste dostupnost ličnih podataka velikom broju ljudi izvan privatne sfere pojedinca. Na osnovu sudske prakse u okviru Direktive o zaštiti podataka, pravo zaštite podataka primenjuje se kada pojedinac prilikom upotrebe interneta objavljuje podatke o drugima na javnoj internet stranici. SPEU još nije odlučivao o sličnim činjenicama na osnovu OUZP-a, koji pruža više smernica o temama za koje se može smatrati da izlaze iz okvira oblasti primene zakona o zaštiti podataka u sklopu „izuzeća za kućne aktivnosti", poput upotrebe društvenih mreža u lične svrhe.

Primer: Predmet *Bodil Lindqvist*[215] odnosio se na upućivanje na različite osobe na internet stranici navođenjem njihovog imena ili na druge načine, na primer, navođenjem njihovog telefonskog broja ili informacija o njihovim hobijima. SPEU je zaključio da „navođenje različitih osoba na internet stranici i njihovo identifikovanje putem imena i prezimena ili na drugi način [...] predstavlja, podatke koji se u celosti ili delimično obrađuju automatskim putem'" u smislu člana 3. stav 1. Direktive o zaštiti podataka[216].

210 Opšta uredba o zaštiti podataka, uvodna izjava 18.

211 *Ibid*., uvodna izjava 18; Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 29.

212 Vidi izjavu Radne grupe iz člana 29. o raspravama o paketu reformi za zaštitu podataka (2013.), *Annex 2: Proposals and Amendments regarding exemption for personal or household activities* (Prilog 2: Predlozi i izmene u pogledu izuzeća za lične ili domaće aktivnosti), 27. februara 2013.

213 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 28.

214 Vidi Opštu uredbu o zaštiti podataka, uvodna izjava 18 i Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 27.

215 SPEU, C-101/01, *Krivični postupak protiv Bodil Lindqvist,* 6. novembra 2003.

216 *Ibid*., stav 27.; nekadašnja Direktiva 95/46/EZ, član 3. tačka (1), sada Opšta uredba o zaštiti podataka, član 2. stav 1.

Takva obrada ličnih podataka ne spada u aktivnosti isključivo lične ili domaće prirode, koje su izvan oblasti primene propisa EU o zaštiti podataka, jer takav izuzetak „treba tumačiti kao da se odnosi isključivo na aktivnosti koje su deo privatnog ili porodičnog života pojedinaca, što očigledno nije slučaj s obradom ličnih podataka koja podrazumeva njihovu objavu na internetu tako da se pristup tim podacima omogući neodređenom broju osoba"[217].

Prema SPEU-u, vizuelni snimci snimljeni privatno postavljenom sigurnosnom kamerom u određenim okolnostima takođe mogu biti obuhvaćene pravom EU o zaštiti podataka.

Primer: U predmetu *František Ryneš*[218] g. Rineš snimio je sliku dveju osoba koje su razbile prozore na njegovom domu, pomoću kućnog sistema video-nadzora s televizijom zatvorenog kruga (CCTV) koji je postavio radi zaštite svoje imovine. Snimak je zatim predat policiji i upotrebljen u krivičnom postupku.

SPEU je izjavio da „[u] meri u kojoj video-nadzor [...] obuhvata, iako delimično, javni prostor, pa je zbog te činjenice usmeren prema eksterijeru privatne sfere onoga ko sprovodi obradu podataka tim sredstvom, ta se obrada ne može smatrati isključivo 'ličnom ili domaćom' aktivnošću [...]"[219].

Rukovalac podacima

Na osnovu prava EU, rukovalac podacima se definiše kao neko ko „sam ili zajedno s drugima određuje svrhe i sredstva obrade ličnih podataka"[220]. Odlukom rukovaoca podacima utvrđuje se zašto se i kako podaci obrađuju.

Na osnovu prava Saveta Evrope, u modernizovanoj Konvenciji br. 108 „rukovalac podacima" definiše se kao „fizičko ili pravno lice, javni organ, služba, agencija ili bilo koje drugo tielo koje samo ili zajedno s drugima ima ovlašćenje da donosi odluke o obradi podataka"[221]. Takvo ovlašćenje da donosi odluke odnosi se na svrhe i načine

217 SPEU, C-101/01, *Krivični postupak protiv Bodil Lindqvist*, 6. novembra 2003, t. 47.

218 SPEU, C-212/13, *František Ryneš protiv Úřad pro ochranu osobních údajů*, 11. decembra 2014, stav 33.

219 Nekadašnja Direktiva 95/46/EZ, član 3. stav 2. druga alineja, sada Opšta uredba o zaštiti podataka, član 2. stav 2. tačka (c).

220 Opšta uredba o zaštiti podataka, član 4. stav 7.

221 Modernizovana Konvencija br. 108, član 2. tačka (d).

obrade, kao i na kategorije podataka koji se obrađuju kao i pristup podacima[222]. Da li se to ovlašćenje zasniva na zakonitom imenovanju ili činjeničnim okolnostima mora se odlučiti u svakom pojedinačnom slučaju[223].

Primer: Postupak u slučaju *Google Spain*[224] pokrenuo je građanin Španije koji je hteo da se stari novinski izveštaj o njegovoj finansijskoj prošlosti ukloni iz pretraživača Gugl.

SPEU je trebalo da odluči da li je kompanija Gugl, kao operater internet pretraživača, „rukovalac podacima" u smislu člana 2. tačka (d) Direktive o zaštiti podataka[225]. SPEU je smatrao da se širokom definicijom pojma „rukovaoca podacima" obezbeđuje „delotvorna i potpuna zaštita ispitanika"[226]. SPEU je zaključio da operater internet pretraživača određuje svrhe i načine te aktivnosti i da podatke koje na internet stranice učitavaju izdavači internet stranica stavlja na raspolaganje svakom korisniku interneta koji vrši pretragu prema imenu ispitanika[227]. Stoga je utvrdio da se kompanija Gugl može smatrati „rukovaocem podacima"[228].

Kada rukovalac podacima ili obrađivač podataka ima sedište izvan EU, ta kompanija mora pisanim putem da imenuje predstavnika unutar EU[229]. U OUZP-u se ističe da predstavnik mora imati sedište „u jednoj od država članica u kojoj se nalaze ispitanici čiji se lični podaci obrađuju u vezi sa robom ili uslugama koje im se nude ili čije se ponašanje prati"[230]. Ako se ne imenuje predstavnik, ipak se može pokrenuti sudski postupak protiv samog rukovaoca podacima ili obrađivača podataka[231].

222 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 22.

223 *Ibid*.

224 SPEU, C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González*a [VV], 13. maja 2014.

225 Opšta uredba o zaštiti podataka, član 4. stav 7.; SEU, C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González*a [VV], 13. maja 2014, stav 21.

226 SPEU, C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González*a [VV], 13. maja 2014, stav 34.

227 *Ibid*., st. od 35 do 40.

228 *Ibid*., stav 41.

229 Opšta uredba o zaštiti podataka, član 27. stav 1.

230 *Ibid*., član 27. stav 3.

231 *Ibid*., član 27. stav 5.

Zajednički nadzor

OUZP-om se propisuje da se dva ili više rukovalaca podacima koji zajednički određuju svrhu i načine obrade smatraju zajedničkim rukovaocima. To znači da zajedno odlučuju o obradi podataka u zajedničke svrhe[232]. U Izveštaju s objašnjenjima o modernizovanoj Konvenciji br. 108 navodi se da je više rukovalaca podacima ili zajedničko vođenje obrade moguće i u **[pravnom] okviru Saveta Evrope**[233].

Radna grupa iz člana 29. ističe da zajedničko vođenje obrade može primiti različite oblike i da učestvovanje različitih rukovalaca podacima u aktivnostima rukovanja podacima može biti nejednako[234]. Takva fleksibilnost omogućava sve složeniju obradu podataka[235]. Stoga zajednički rukovaoci podacima moraju u posebnom ugovoru odrediti svoje pojedinačne odgovornosti za usklađenost sa obavezama na osnovu Uredbe[236].

Zajedničko rukovanje podacima dovodi do zajedničke odgovornosti za aktivnost obrade[237]. U okviru **prava EU** to znači da svaki rukovalac podacima ili obrađivač podataka može biti potpuno odgovoran za celu štetu uzrokovanu obradom pod zajedničkim rukovanjem podacima kako bi se obezbedilo da ispitanik dobije odgovarajuću naknadu[238].

Primer: Uobičajen primer zajedničkog rukovanja podacima jeste baza podataka koju za svoje klijente, koji ne ispunjavaju obaveze, zajednički vodi nekoliko kreditnih institucija. Kada osoba zatraži kredit od banke koja je jedna od zajedničkih rukovalaca podacima, banke proveravaju bazu podataka radi lakšeg donošenja odluke na osnovu primljenih informacija o kreditnoj sposobnosti podnosioca zahteva.

232 *Ibid*., član 4. stav 7. i član 26.

233 Modernizovana Konvencija br. 108, član 2. tačka (d); Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 22.

234 Radna grupa iz člana 29. (2010), *Opinion 1/2010 on the concepts of „controller" and „processor"* (Mišljenje 1/2010 o pojmovima „rukovalac podacima" i „obrađivač podataka"), WP 169, Bruxelles, 16. februara 2010, str. 19.

235 *Ibid*.

236 Opšta uredba o zaštiti podataka, uvodna izjava 79.

237 *Ibid*., t. 21.

238 *Ibid*., član 82. stav 4.

U zakonskim odredbama ne navodi se izričito da li zajedničko rukovanje podacima zahteva da zajednička svrha bude ista za svakog rukovaoca podacima ili je dovoljno da se njihove svrhe tek delimično preklapaju. Na evropskom nivou zasad nema relevantne sudske prakse. U Mišljenju iz 2010. o rukovaocima podacima i obrađivačima podataka Radna gupa iz člana 29. navodi da zajednički rukovaoci podacima mogu deliti sve svrhe i načine obrade ili mogu deliti samo neke svrhe ili načine ili njihove delove[239]. Dok bi ovo prvo podrazumevalo vrlo blizak odnos između različitih učesnika, drugo bi ukazivalo na manje blizak odnos.

Radna grupa iz člana 29. zagovara šire tumačenje pojma zajedničkog nadzora u cilju fleksibilnosti kojom bi se odgovorilo na sve složeniju trenutnu situaciju po pitanju obrade podataka[240]. Slučaj u koji je bilo uključeno Društvo za svetsku međubankovnu financijsku telekomunikaciju (Society for Worldwide Interbank Financial Telecommunication, SWIFT) ilustruje stav Radne grupe.

Primer: U takozvanom predmetu SWIFT, evropske bankovne institucije angažovale su SWIFT, prvobitno kao rukovaoca podacima, za operacije prenosa podataka tokom bankovnih transakcija. SWIFT je te podatke o bankovnim transakcijama, pohranjene u računarskom uslužnom centru u Sjedinjenim Američkim Državama (SAD), otkrio Ministarstvu finansija SAD iako mu to nisu izričito naložile evropske bankarske institucije koje su ga angažovale. Prilikom procene zakonitosti ove situacije, Radna grupa iz člana 29 zaključila je da na evropske bankarske institucije koje su angažovale SWIFT, kao i na sam SWIFT, treba gledati kao na zajedničke rukovaoce podacima koji evropskim klijentima odgovaraju za otkrivanje njihovih podataka nadležnim telima SAD[241].

Obrađivač podataka

„Obrađivač podataka" se **na osnovu prava EU** definiše kao osoba koja obrađuje lične podatke u ime rukovaoca podacima[242]. Aktivnosti poverene obrađivaču podataka

239 Radna grupa iz člana 29. (2010), *Opinion 1/2010 on the concepts of „controller" and „processor"* (Mišljenje 1/2010 o pojmovima „rukovalac podacima" i „obrađivač podataka"), WP 169, Bruxelles, 16. februara 2010, str. 19.

240 *Ibid*.

241 Radna grupa iz člana 29. (2006), *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)* (Mišljenje 10/2006 o obradi ličnih podataka od strane Društva za svetsku međubankovnu finansijsku telekomunikaciju (SWIFT)), WP 128, Bruxelles, 22. novembra 2006.

242 Opšta uredba o zaštiti podataka, član 4. stav 8.

mogu se ograničiti na vrlo konkretan zadatak ili kontekst ili mogu biti prilično uopštene i sveobuhvatne.

Na osnovu prava Saveta Evrope značenje pojma obrađivača podataka isto je kao i prema pravu Unije[243].

Osim što obrađuju podatke za druge, obrađivači podataka su takođe i rukovaoci podacima s obzirom na obradu podataka koju vrše u sopstvene svrhe, na primer, upravljanje sopstvenim zaposlenima, platama i računima.

Primer: Društvo Everready specijalizovano je za obradu podataka radi upravljanja podacima o ljudskim potencijalima za druga društva. U toj funkciji Everready je obrađivač podataka. Međutim, kada društvo Everready obrađuje podatke svojih zaposlenih, ono je rukovalac podacima za postupke obrade podataka jer time ispunjava svoje obaveze kao poslodavac.

Odnos između rukovaoca podacima i obrađivača podataka

Kao što je rečeno, rukovalac podacima je definisan kao onaj koji utvrđuje svrhu i načine obrade. U OUZP-u se jasno navodi da obrađivač podataka sme da obrađuje lične podatke samo po uputstvu rukovaoca podacima, osim ako je zakonima EU ili države članice propisano da to obrađivač podataka čini[244]. Ugovor između rukovaoca podacima i obrađivača podataka je osnovni element njihovog odnosa i predstavlja zakonsku obavezu[245].

Primer: Direktor kompanije Sunshine odlučio je da kompaniju Cloudy, specijalano za čuvanje podataka u klaudu, upravlja podacima o kupcima kompanije Sunshine. Kompanija Sunshine ostaje rukovalac podacima, a kompanija Cloudy samo je obrađivač podataka jer, prema ugovoru, Cloudy može da upotrebljava podatke o kupcima kompanije Sunshine samo u svrhe koje utvrdi Sunshine.

Ako se ovlašćenje utvrđivanja načina obrade poveri obrađivaču podataka, rukovalac podacima svejedno mora da primeni odgovarajući nivo nadzora nad odlukama

243 Modernizovana Konvencija br. 108, član 2. tačka (f).

244 Opšta uredba o zaštiti podataka, član 29.

245 *Ibid*., član 28. stav 3.

obrađivača podataka u pogledu načina obrade. Sveukupna odgovornost ostaje na strani rukovaoca podacima, koji mora da nadgleda obrađivača podataka kako bi obezbedio da njihove odluke budu u skladu sa zakonom o zaštiti podataka i njegovim sopstvenim uputstvima.

Zatim, u slučaju da obrađivač podataka ne poštuje uslove obrade podataka na način koji propiše rukovalac podacima, obrađivač podataka bi postao rukovalac podacima bar u opsegu kršenja uputstva rukovaoca podacima. U tom slučaju će obrađivač podataka najverovatnije postati rukovalac podacima koji deluje nezakonito, a prvobitni rukovalac podacima moraće da objasni kako je obrađivač podataka mogao da prekrši svoje ovlašćenje[246]. Radna grupa iz člana 29. zaista često pretpostavlja da su takvi slučajevi stvar zajedničkog nadzora jer je to u najboljem interesu zaštite ispitanika[247].

Pitanje o podeli odgovornosti može se javiti i kada je rukovalac podacima malo preduzeće, a obrađivač podataka velika korporacija koja može da diktira uslove usluga koje pruža. U takvim okolnostima Radna grupa iz člana 29. smatra da se standard odgovornosti ne sme spuštati zbog ekonomske nejednakosti i da se mora zadržati shvatanje pojma rukovaoca podacima[248].

Radi jasnoće i transparentnosti, pojedinosti odnosa rukovaoca podacima i obrađivača podataka moraju se urediti pisanim ugovorom[249]. Ugovor mora posebno uključivati predmet, prirodu, svrhu i trajanje obrade, vrstu ličnih podataka i kategorije ispitanika. U njemu takođe treba da budu utvrđene obaveze i prava rukovaoca podacima i obrađivača podataka, kao što je zahtev u vezi sa poverljivošću i bezbednošću. U suprotnom se krši obaveza rukovaoca podacima u pogledu predstavljanja pisane dokumentacije o uzajamnim odgovornostima, što može dovesti do kazni. Kada šteta nastane kao posledica delovanja izvan zakonitih uputstava rukovaoca podacima ili njihovog nepridržavanja, ne snosi odgovornost samo rukovalac podacima, nego i obrađivač podataka[250]. Obrađivač podataka mora da vodi evidenciju o

246 *Ibid*., član 82. stav 2.

247 Radna grupa iz člana 29. (2010), *Mišljenje 1/2010 o pojmovima „rukovalac podacima" i „obrađivač podataka"*, WP 169, Bruxelles, 16. februara 2010, str. 25.; Radna grupa iz člana 29. (2006.), Mišljenje 10/2006 o obradi ličnih podataka od strane Društva za svetsku međubankovnu finansijsku telekomunikaciju (SWIFT), WP 128, Bruxelles, 22. novembra 2006.

248 Radna grupa iz člana 29. (2010), Opinion 1/2010 on the concepts of „controller" and „processor" (Mišljenje 1/2010 o pojmovima „rukovalac podacima" i „obrađivač podataka"), WP 169, Bruxelles, 16. februara 2010, str. 26.

249 Opšta uredba o zaštiti podataka, član 28. stav 3. i član 9.

250 *Ibid*., član 82. stav 2.

svim kategorijama aktivnosti obrade koje sprovodi u ime rukovaoca podacima[251]. Ta evidencija mora biti dostupna na zahtev nadzornog organa budući da i rukovalac podacima i obrađivač podataka moraju da sarađuju s tim telom u obavljanju svojih zadataka[252]. Rukovaoci podacima i obrađivači podataka takođe imaju mogućnost da se pridržavaju odobrenog kodeksa ponašanja ili mehanizma sertifikovanja kako bi dokazali usklađenost sa zahtevima iz OUZP-a[253].

Obrađivači podataka mogu prepustiti određene zadatke podizvršiocima. To je pravno dopustivo, pod uslovom da se utvrde odgovarajuće ugovorne odredbe između rukovaoca podacima i obrađivača podataka, uključujući činjenicu da li je ovlašćenje rukovaoca podacima nužno u svakom pojedinačnom slučaju ili je dovoljno samo obaveštenje. U OUZP-u je utvrđeno da početni obrađivač podataka ostaje u celini odgovoran rukovaocu podacima ako podobrađivač podataka ne ispuni svoje obaveze zaštite podataka[254].

Prema pravu Saveta Evrope, u potpunosti je primenjivo tumačenje pojmova rukovaoca podacima i obrađivača podataka, kako je prethodno opisano[255].

2.3.2. Primaoci i treće strane

Razlika između ove dve kategorije lica ili subjekata, uvedene Direktivom o zaštiti podataka, uglavnom se odnosi na odnos koji imaju sa rukovaocem podacima, a time na ovlašćenje za pristup ličnim podacima navedenog rukovaoca podacima.

„Treća strana" je osoba koja se razlikuje od rukovaoca podacima i obrađivača podataka. Prema članu 4 stav 10. OUZP-a, treća strana je „fizičko ili pravno lice, organ javne vlasti, agencija ili drugo telo koje nije ispitanik, rukovalac podacima, obrađivač podataka i lica koja su ovlašćena za obradu ličnih podataka pod neposrednom nadležnošću rukovaoca podacima i obrađivača podataka". To znači da će lica koja rade za organizaciju koja se razlikuje od rukovaoca podacima – čak i ako pripada istoj grupaciji ili holdingu – biti „treća strana" (ili će joj pripadati). S druge strane,

251 *Ibid.*, član 30. stav 2.

252 *Ibid.*, član 30. stav 4. i član 31.

253 *Ibid.*, član 28. stav 5. i član 4. stav 4.

254 *Ibid.*, član 28. stav 4.

255 Na primer, videti modernizovanu Konvenciju br. 108, član 2. tačke (b) i (f); Preporuku o izradi profila, član 1.

poslovnice banke koje obrađuju račune klijenata pod neposrednim ovlašćenjem svojih sedišta neće se smatrati „trećim stranama"[256].

„Primalac" je širi pojam od pojma „treća strana". U smislu člana 4. stav 9. OUZP-a, primalac je „fizičko ili pravno lice, organ javne vlasti, agencija ili drugo telo kojem se otkrivaju lični podaci, nezavisno od toga da li je on treća strana". Primalac može biti ili lice izvan rukovaoca podacima ili obrađivača podataka – u tom slučaju je to treća strana – ili neko unutar rukovaoca podacima ili obrađivača podataka, kao što je zaposleni ili drugi odsek unutar istog društva ili tela.

Razlika između primaoca i trećih strana važna je samo zbog uslova za zakonito otkrivanje podataka. Zaposleni rukovaoca podacima ili obrađivača podataka mogu da budu primaoci ličnih podataka bez dodatnih pravnih zahteva ako su uključeni u postupke obrade rukovaoca podacima ili obrađivača podataka. S druge strane, s obzirom na to da je treća strana zaseban subjekt u odnosu na rukovaoca podacima ili obrađivača podataka, ona nije ovlašćena da upotrebljava lične podatke koje obradi rukovalac podacima, osim ako za to u konkretnom slučaju postoje konkretne pravne osnove.

Primer: Zaposleni rukovaoca podacima koji upotrebljava lične podatke u okviru zadataka koje mu je poverio poslodavac primalac je podataka, ali nije treća strana, jer upotrebljava podatke u ime i prema uputstvima rukovaoca podacima. Na primer, ako poslodavac otkrije lične podatke svojih zaposlenih svom odseku ljudskih resursa radi nadolazećih procena radnog učinka, osoblje ljudskih resursa biće primaoci ličnih podataka budući da su podaci njima otkriveni tokom obrade za rukovaoca podacima.

Međutim, ako organizacija da podatke o svojim zaposlenima društvu za obuke, koje će upotrebiti podatke da bi prilagodilo program obuka zaposlenima, to društvo je treća strana. To je zato što društvo koje vodi obuke nema posebnu legitimnost ili ovlašćenje (koje u slučaju „ljudskih resursa" proizlazi iz radnog odnosa s rukovaocem podacima) za obradu tih ličnih podataka. Drugim rečima, društvo nije dobilo te informacije u sklopu zaposlenja kod rukovaoca podacima.

256 Radna grupa iz člana 29. (2010), *Opinion 1/2010 on the concept of „controller" and „processor"* (Mišljenje 1/2010 o pojmovima „rukovalac podacima" i „obrađivač podataka"), WP 169, Bruxelles, 16. februara 2010, str. 31.

2.4. Pristanak/Saglasnost

Ključne tačke

- Pristanak kao pravna osnova za obradu ličnih podataka mora biti dobrovoljno dat, utemeljen na informacijama, poseban i nedvosmislen znak želje potvrđen jasnim činom koji predstavlja pristajanje na obradu.
- Za obradu posebnih kategorija podataka potreban je izričit pristanak.

Kao što se detaljno razmatra u poglavlju 4, pristanak je jedna od šest legitimnih pravnih osnova za obradu ličnih podataka. Pristanak znači „svako dobrovoljno, posebno, informisano i nedvosmisleno izražavanje želja ispitanika"[257].

Pravom EU propisuje se nekoliko elemenata koji su preduslovi da bi pristanak bio vežeći. Njima se garantuje da su ispitanici zaista pristali na određenu upotrebu svojih podataka[258]:

- Pristanak se mora dati jasnim potvrdnim činom kojim se daje dobrovoljan, poseban, nedvosmislen znak, utemeljen na informacijama, da je ispitanik saglasan sa obradom svojih podataka. Takav čin može biti radnja ili izjava.
- Ispitanik mora imati pravo na povlačenje pristanka u svakom trenutku.
- U kontekstu pisane izjave koja obuhvata i druga pitanja, poput „uslova pružanja usluge", zahtevi za pristanak moraju biti sastavljeni na jasan i jednostavan način i imati razumljiv i lako dostupan oblik, kojim se pristanak jasno razlikuje od drugih pitanja. Ako se bilo kojim delom te izjave krši OUZP, ona nije obavezujuća.

Pristanak je važeći u kontekstu zakona o zaštiti podataka samo ako su ispunjeni svi ovi uslovi. Odgovornost rukovaoca podacima je da dokaže da je ispitanik pristao na obradu svojih podataka[259]. Elementi važećeg pristanka dodatno se razmatraju u delu 4.1.1. o zakonitim osnovama obrade ličnih podataka.

257 Opšta uredba o zaštiti podataka, član 4. stav 11. Videti i modernizovanu Konvenciju br. 108, član 5. stav 2.

258 Opšta uredba o zaštiti podataka, član 7.

259 *Ibid.*, član 7. stav 1.

Konvencija br. 108 ne sadrži definiciju pristanka; to je prepušteno domaćim zakonodavstvima. Međutim, **u skladu sa pravom Saveta Evrope**, elementi važećeg pristanka odgovaraju prethodno opisanima[260].

Dodatni zahtevi za važeći pristanak u okviru građanskog prava, kao što je pravna sposobnost, takođe se primenjuju u kontekstu zaštite podataka jer su takvi zahtevi osnovni pravni preduslovi. Nevažeći pristanak lica bez pravne sposobnosti podrazumeva nedostatak pravne osnove za obradu podataka o takvim licima. Kad je reč o pravnoj sposobnosti maloletnika za sklapanje ugovora, OUZP-om se propisuje da njene odredbe o najnižem uzrastu za dobijanje važećeg pristanka ne utiču na opšte ugovorno pravo država članica[261].

Pristanak se mora dati na jasan način, tako da se ne dovode u sumnju namere ispitanika[262]. Pristanak mora biti izričit kada se odnosi na obradu osetljivih podataka, a može se dati usmeno ili pisanim putem[263]. Pisana saglasnost se može dati elektronskim putem[264]. U okviru **prava EU** i **Saveta Evrope**, pristanak na obradu nečijih ličnih podataka mora se dati izjavom ili jasnim potvrdnim činom[265]. Stoga se pristanak ne može dobiti na osnovu tišine, unapred označenih potvrdnih okvira, unapred ispunjenih obrazaca ili neaktivnosti[266].

260 Modernizovana Konvencija br. 108, član 5. stav 2.; Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stavovi od 42 do 45.

261 Opšta uredba o zaštiti podataka, član 8. stav 3.

262 *Ibid*., član 6. stav 1. tačka (a) i član 9. stav 2. tačka (a).

263 *Ibid*., uvodna izjava 32.

264 *Ibid*.

265 *Ibid*., član 4. stav 11.; Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 42.

266 Opšta uredba o zaštiti podataka, uvodna izjava 32; Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 42.

3

Glavna načela evropskog prava zaštite podataka

EU	Obuhvaćena pitanja	Savet Evrope
Opšta uredba o zaštiti podataka, član 5. stav 1. tačka (a)	**Načelo zakonitosti**	Modernizovana Konvencija br. 108, član 5. stav 3.
Opšta uredba o zaštiti podataka, član 5. stav 1. tačka (a)	**Načelo pravičnosti**	Modernizovana Konvencija br. 108, član 5. stav 4. tačka (a) ESLJP, *K. H. i drugi protiv Slovačke*, br. 32881/04, 2009.
Opšta uredba o zaštiti podataka, član 5. stav 1. tačka (a) SPEU, C-201/14, *Smaranda Bara i dr. protiv Casa Națională de Asigurări de Sănătate i dr.*, 2015.	**Načelo transparentnosti**	Modernizovana Konvencija br. 108, član 5. stav 4. tačka (a) i član 8. ESLJP, *Haralambie protiv Rumunije*, br. 21737/03, 2009.
Opšta uredba o zaštiti podataka, član 5. stav 1. tačka (b)	**Načelo ograničenja svrhe**	Modernizovana Konvencija br. 108, član 5. stav 4. tačka (b)
Opšta uredba o zaštiti podataka, član 5. stav 1. tačka (c) SPEU, spojeni predmeti C-293/12 i C-594/12 *Digital Rights Ireland* i *Kärntner Landesregierung i dr.* [VV], 2014.	**Načelo smanjenja količine podataka**	Modernizovana Konvencija br. 108, član 5. stav 4. tačka (c)
Opšta uredba o zaštiti podataka, član 5. stav 1. tačka (d) SPEU, C-553/07, *College van burgemeester en wethouders van Rotterdam protiv M. E. E. Rijkeboer*, 2009.	**Načelo tačnosti podataka**	Modernizovana Konvencija br. 108, član 5. stav 4. tačka (d)

EU	Obuhvaćena pitanja	Savet Evrope
Opšta uredba o zaštiti podataka, član 5. stav 1. tačka (e) SPEU, spojeni predmeti C-293/12 i C-594/12 *Digital Rights Ireland* i *Kärntner Landesregierung i dr.* [VV], 2014.	**Načelo ograničenja čuvanja**	Modernizovana Konvencija br. 108, član 5. stav 4. tačka (e) ESLJP, *S. i Marper protiv Ujedinjenog Kraljevistva* [VV], br. 30562/04 i 30566/04, 2008.
Opšta uredba o zaštiti podataka, član 5. stav 1. tačka (f) i član 32.	**Načelo bezbednosti (celovitosti i poverljivosti) podataka**	Modernizovana konvencija br. 108, član 7.
Opšta uredba o zaštiti podataka, član 5. stav 2.	**Načelo odgovornosti**	Modernizovana Konvencija br. 108, član 10.

U članu 5. Opšte uredbe o zaštiti podataka utvrđuju se načela kojima se reguliše obrada ličnih podataka. Ta načela obuhvataju sledeće:

- zakonitost, pravičnost i transparentnost,
- ograničenje svrhe,
- smanjenje količine podataka,
- tačnost podataka,
- ograničavanje čuvanja,
- celovitost i poverljivost.

Načela služe kao polazište za detaljnije odredbe u narednim članovima Uredbe. Javljaju se i u članovima 5., 7., 8. i 10. modernizovane Konvencije br. 108. Svi kasnije propisi o zaštiti podataka na nivou Saveta Evrope ili Evropske unije moraju da budu u skladu s tim načelima i moraju se uzeti u obzir pri tumačenju tih propisa. Prema pravu EU, ograničenja načela obrade dopuštena su samo u meri u kojoj odgovaraju pravima i obavezama iz člana od 12 do 22 i moraju da budu u skladu sa suštinom osnovnih prava i sloboda. Sva izuzeća i ograničenja u pogledu tih ključnih načela moraju biti propisana na nivou EU ili domaćem nivou[267], moraju biti zakonom pro-

267 Modernizovana Konvencija br. 108, član 11. stav 1.; Opšta uredba o zaštiti podataka, član 23. stav 1.

pisana, imati legitimnu svrhu i biti nužne i srazmerne mere u demokratskom društvu[268]. Sva tri uslova moraju biti ispunjena.

3.1. Načela zakonitosti, pravičnosti i transparentnosti obrade

Ključne tačke

- Načela zakonitosti, pravičnosti i transparentnosti primenjuju se na svu obradu ličnih podataka.
- Prema OUZP-u, za zakonitost je potrebno nešto od sledećeg:
  - pristanak ispitanika,
  - nužnost sklapanja ugovora,
  - zakonska obaveza,
  - nužnost zaštite vitalnih interesa ispitanika ili druge osobe,
  - nužnost izvršavanja zadatka od javnog interesa,
  - nužnost legitimnih interesa rukovaoca podacima ili treće strane ako nisu nadjačani interesima i pravima ispitanika.
- Obrada ličnih podataka treba da se vrši na pravičan način.
  - Ispitanik se mora obavestiti o riziku kako bi se obezbedilo da obrada nema nepredviđene neželjene efekte.
- Obrada ličnih podataka treba da se sprovodi na transparentan način.
  - Rukovaoci podacima moraju obavestiti ispitanike pre obrade njihovih podataka, između ostalog i o svrsi obrade i identitetu i adresi rukovaoca podacima.
  - Informacije o postupcima obrade moraju se pružiti na jasan i jednostavan način kako bi ispitanici lako razumeli povezana pravila, rizike, zaštitne mere i prava.
  - Ispitanici imaju pravo pristupa svojim podacima gde god da se oni obrađuju.

268 Opšta uredba o zaštiti podataka, član 23. stav 1.

3.1.1. Zakonitost obrade podataka

Pravom zaštite podataka EU i Saveta Evrope propisano je da se podaci obrađuju na zakonit način[269]. Za zakonitu obradu potreban je pristanak ispitanika ili druga legitimna osnova utvrđena zakonodavstvom o zaštiti podataka[270]. U članu 6. stav 1. OUZP-a navedeno je pet zakonitih osnova obrade osim pristanka, odnosno: kada je obrada ličnih podataka nužna za izvršavanje ugovora, za izvršavanje zadatka na koje je ovlašćeno javno telo, za poštovanje pravne obaveze, za potrebe legitimnih interesa rukovaoca podacima ili trećih strana ili za zaštitu ključnih interesa ispitanika ako je potrebno. To je detaljnije objašnjeno u delu 4.1.

3.1.2. Pravičnost u obradi podataka

Uz zakonitu obradu, zakonima o zaštiti podataka EU i Saveta Evrope propisano je da se podaci obrađuju na pravičan način[271]. Načelom pravične obrade prvenstveno se uređuje odnos rukovaoca podacima i ispitanika.

Rukovaoci podacima trebalo bi da obaveste ispitanike i javnost o tome da će obraditi podatke na zakonit i transparentan način i moraju da imaju moć da dokažu usklađenost postupaka obrade s OUZP-om. Postupci obrade ne smeju se sprovoditi u tajnosti i ispitanici treba da budu svesni mogućih rizika. Osim toga, rukovaoci podacima moraju postupati na način koji što više odgovara željama ispitanika, pogotovo ako njegov pristanak predstavlja pravnu osnovu za obradu podataka.

Primer: U predmetu *K. H. i drugi protiv Slovačke*[272] podnositeljke predstavki su bile žene romskog etničkog porekla koje su tokom trudnoće i porođaja boravile u dvema bolnicama u istočnoj Slovačkoj. Posle toga nijedna od njih nije mogla ponovo da začne dete uprkos uzastopnim pokušajima. Domaći sudovi su bolnicama naložili da podnositeljkama predstavki i njihovim zastupnicima dopuste uvid u njihove zdravstvene kartone i prepisivanje delova iz njih, ali odbacili su njihov zahtev da fotokopiraju dokumenta navodno zbog sprečavanja

269 Modernizovana Konvencija br. 108, član 5. stav 3.; Opšta uredba o zaštiti podataka, član 5. stav 1. tačka (a).

270 Povelja Evropske unije o temeljnim pravima, član 8. stav 2; Opšta uredba o zaštiti podataka, uvodna izjava 40 i čl. od 6 do 9; modernizovana Konvencija br. 108, član 5. stav 2.; Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 41.

271 Opšta uredba o zaštiti podataka, član 5. stav 1. tačka (a); modernizovana Konvencija br. 108, član 5. stav 4. tačka (a).

272 ESLJP, *K. H. i drugi protiv Slovačke*, br. 32881/04, 28. aprila 2009.

zloupotrebe. Iz pozitivnih obaveza država iz člana 8. EKLJP-a proizlazila je dužnost da se ispitanicima stave na raspolaganje kopije dosijea s njihovim podacima. Na državi je bilo da odredi načine kopiranja dosijea s ličnim podacima ili, ako je to prikladno, navede uverljive razloge za uskraćivanje kopiranja. U slučaju podnositeljki predstavki, domaći sudovi su zabranu kopiranja zdravstvenih kartona prvenstveno opravdali potrebom da se odgovarajuće informacije zaštite od zloupotrebe. Međutim, ESLJP nije mogao da shvati kako bi podnositeljke predstavki, koje su ionako dobile pristup celokupnoj zdravstvenoj dokumentaciji, mogle zloupotrebiti informacije o sebi. Osim toga, rizik od takve zloupotrebe mogao se sprečiti na drugačiji način umesto zabranom podnositeljkama predstavki da kopiraju dosijee, na primer, ograničenjem opsega osoba koje imaju pravo pristupa dosijeima. Država nije uspela da iznese dovoljno uverljive razloge zbog kojih je podnositeljkama predstavki zabranjen delotvoran pristup informacijama o njihovom zdravlju. ESLJP je zato zaključio da je došlo do povrede člana 8. Konvencije.

Što se tiče internet usluga, svojstva sistema za obradu podataka moraju omogućiti ispitanicima da zaista razumeju šta se događa sa njihovim podacima. U svakom slučaju, načelo pravičnosti nadilazi obavezu transparentnosti i može se takođe povezati sa etičkom obradom ličnih podataka.

Primer: Istraživački odsek univerziteta izvodi eksperiment u kojem analizira promene raspoloženja 50 ispitanika. Ispitanici moraju da zabeleže svoja razmišljanja u elektronsku datoteku svakog sata u određeno vreme. Tih 50 osoba je dalo pristanak za taj konkretni projekat i tu konkretnu upotrebu podataka u sklopu univerziteta. Istraživački odsek uskoro otkriva da bi elektronsko beleženje razmišljanja bilo vrlo korisno za drugi projekat usmeren na mentalno zdravlje pod vođstvom drugog tima. Iako je univerzitet kao rukovalac podacima mogao da upotrebi iste podatke za rad drugog tima bez dodatnih koraka za obezbeđivanje zakonitosti obrade tih podataka, budući da su svrhe usklađene, univerzitet je obavestio ispitanike i zatražilo nov pristanak u skladu sa svojim etičkim kodeksom u istraživanjima i načelu pravične obrade.

3.1.3. Transparentnost obrade podataka

Pravom zaštite podataka EU i Saveta Evrope zahteva se da lični podaci budu „transparentno obrađivani s obzirom na ispitanika"[273].

Tim načelom se utvrđuje obaveza rukovaoca podacima da preduzme sve odgovarajuće mere kako bi ispitanici, koji mogu biti korisnici, kupci ili klijenti, bili obavešteni o načinu upotrebe njihovih podataka[274]. Transparentnost se može odnositi na informacije date pojedincu pre početka obrade[275], informacije koje treba da budu dostupne ispitanicima tokom obrade[276] i informacije date ispitanicima nakon njihovog zahteva za pristup sopstvenim podacima[277].

> Primer: U predmetu *Haralambie protiv Rumunije*[278] podnosiocu predstavke je dopušten pristup informacijama koje je organizacija tajne službe čuvala u vezi s njim tek pet godina nakon njegovog zahteva. ESLJP je ponovio da je od vitalne važnosti da pojedinci o kojima javni organi čuvaju lične dosijee mogu pristupiti takvim dosijeima. Organi su bili dužni da obezbede delotvoran postupak dobijanja pristupa takvim informacijama. ESLJP je smatrao da ni količina prenesenih dosijea, niti nedostaci sistema arhiviranja, nisu opravdavali petogodišnje kašnjenje odobravanja zahteva za pristup dosijeima podnosioca predstavke. Organi nisu obezbedili delotvoran i pristupačan postupak kojim bi se podnosiocu predstavke omogućio pristup ličnim dosijeima u razumnom roku. ESLJP je stoga zaključio da je došlo do povrede člana 8. Konvencije.

Postupci obrade moraju se objasniti ispitanicima na jednostavan i pristupačan način kako bi im se omogućilo da razumeju šta će se dogoditi s njihovim podacima. To znači da konkretna svrha obrade ličnih podataka mora biti poznata ispitaniku u trenutku prikupljanja ličnih podataka[279]. Transparentnost obrade podataka zahteva

273 Opšta uredba o zaštiti podataka, član 5. stav 1. tačka (a); modernizovana Konvencija br. 108, član 5. stav 4. tačka (a) i član 8.

274 Opšta uredba o zaštiti podataka, član 12.

275 *Ibid.*, članovi 13. i 14.

276 Radna grupa iz člana 29., *Mišljenje 2/2017 o obradi podataka na radnom mestu*, WP 249, str. 23.

277 Opšta uredba o zaštiti podataka, član 15.

278 ESLJP, *Haralambie protiv Rumunije*, br. 21737/03, 27. oktobra 2009.

279 Opšta uredba o zaštiti podataka, uvodna izjava 39.

jasno i jednostavno izražavanje[280]. Dotičnim licima moraju biti jasna pravila, rizici, zaštitne mere i prava u vezi sa obradom njihovih ličnih podataka[281].

U pravu Saveta Evrope takođe je utvrđeno da rukovalac podacima mora obavezno davati određene ključne informacije ispitanicima na proaktivan način. Informacije o imenu i adresi rukovaoca podacima (ili više zajedničkih rukovalaca podacima), pravnoj osnovi i svrhama obrade podataka, kategorijama podataka koji se obrađuju i primaocima, kao i o načinima ostvarivanja prava mogu se dati u bilo kom primerenom obliku (putem internet stranice, tehnoloških alata na ličnim uređajima itd.), pod uslovom da su informacije pravično i stvarno predstavljene ispitaniku. Te informacije moraju biti lako dostupne, čitljive, razumljive i prilagođene pojedinim ispitanicima (na primer, na jeziku prilagođenom deci kada je to potrebno). Potrebno je dati i sve dodatne informacije koje su potrebne da bi se obezbedila pravična obrada podataka ili koje su korisne za takvu svrhu, poput perioda čuvanja, saznanja o razlozima za obradu podataka ili informacija o prenosima podataka primaocu koji pripada drugoj strani ili nije strana (između ostalog, da li osoba koja nije strana daje odgovarajući nivo zaštite ili mere koje preduzima rukovalac podacima kako bi se zagarantovao takav odgovarajući nivo zaštite podataka)[282].

U skladu sa pravom na pristup[283], ispitanik ima pravo da na svoj zahtev sazna od rukovaoca podacima da li se obrađuju njegovi podaci i ako da, koji se podaci obrađuju[284]. Usto, u skladu sa pravom na informisanje[285], rukovalac podacima ili obrađivač podataka moraju proaktivno obavestiti osobe čiji se podaci obrađuju, između ostalog, o svrhama, trajanju i načinima obrade, u načelu pre početka postupka obrade.

Primer: Predmet *Smaranda Bara i dr. protiv Preşedintele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Administrare Fiscală (ANAF)*[286] odnosio se na prenos poreskih podataka u vezi s prihodom od samostalnih delatnosti Državne agencije za poresko upravljanje rumunskom Državnom zavodu za socijalnu bezbednost, na osnovu kojih je zatražena uplata zaostalih

280 *Ibid*.

281 *Ibid*.

282 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 68.

283 Opšta uredba o zaštiti podataka, član 15.

284 Modernizovana Konvencija br. 108, član 8. i član 9. stav 1. tačka (b).

285 Opšta uredba o zaštiti podataka, članovi 13. i 14.

286 SPEU, C-201/14, *Smaranda Bara i dr. protiv Casa Naţională de Asigurări de Sănătate i dr.*, 1. oktobra 2015, st. od 28 do 46.

doprinosa u sistem osiguranja. Od SPEU se tražilo da utvrdi da li je ispitanik trebalo prethodno da dobije informacije o identitetu rukovaoca podacima i svrsi prenosa podataka pre nego što je Državni zavod za socijalnu bezbednost obradio te podatke. SPEU je zaključio da kada organ javne uprave neke države članice prenosi lične podatke drugom organu javne uprave koje dalje obrađuje te podatke, ispitanici moraju biti obavesteni o tom prenosu ili obradi.

U određenim situacijama dopuštena su odstupanja od obaveze informisanja ispitanika o obradi podataka. Odstupanja se dodatno obrađuju u delu 6.1. o pravima ispitanika.

3.2. Načelo ograničenja svrhe

Ključne tačke

- Svrha obrade podataka mora se jasno definisati pre početka obrade.
- Nije dopuštena dalja obrada podataka na način koji nije u skladu s izvornom svrhom, iako su u Opštoj uredbi o zaštiti podataka predviđena izuzeća od tog pravila za svrhe arhiviranja u javnom interesu, naučna ili istorijska istraživanja i statističke analize.
- U suštini, načelo ograničenja svrhe znači da se svaka obrada ličnih podataka mora vršiti u određenu, jasno definisanu svrhu i samo u dodatne utvrđene svrhe koje su usklađene s izvornom.

Načelo ograničenja svrhe je jedno od osnovnih načela evropskog prava zaštite podataka. Uveliko je povezano sa transparentnošću, predvidivošću i korisničkim nadzorom: ako je svrha obrade dovoljno specifična i jasna, pojedinci znaju šta mogu da očekuju i povećavaju se transparentnost i pravna sigurnost. Istovremeno, jasno razgraničenje svrhe važno je kako bi se ispitanicima omogućilo efikasno ostvarivanje njihovih prava, poput prava na prigovor na obradu[287].

Ovim načelom određuje se da se svaka obrada ličnih podataka mora vršiti u određenu, jasno definisanu svrhu i samo u dodatne svrhe koje su usklađene s izvornom[288]. Obrada ličnih podataka u nedefinisane i/ili neograničene svrhe stoga nije

287 Radna grupa iz člana 29. (2013), *Opinion 3/2013 on purpose limitation* (Mišljenje 3/2013 o ograničavanju svrhe), WP 203, 2. aprila 2013.

288 Opšta uredba o zaštiti podataka, član 5. stav 1. tačka (b).

zakonita. Obrada ličnih podataka bez određene svrhe, samo na osnovu mišljenja da bi mogli biti korisni u budućnosti, takođe nije zakonita. Legitimnost obrade ličnih podataka zavisiće od svrhe obrade, koja mora biti izričita, utvrđena i legitimna.

Svaka nova svrha obrade podataka koja nije usklađena s izvornom mora imati sopstvenu posebnu pravnu osnovu i ne može se oslanjati na činjenicu da su podaci prvobitno stečeni ili obrađeni u drugu legitimnu svrhu. Zakonita obrada je ograničena na svoju prvobitno određenu svrhu, pa svaka nova svrha obrade iziskuje novu posebnu pravnu osnovu. Na primer, otkrivanje podataka trećim stranama u novu svrhu mora se pažljivo razmotriti, jer takvo otkrivanje često iziskuje dodatnu pravnu osnovu različitu od one za prikupljanje podataka.

Primer: Avio-kompanija prikuplja podatke od svojih putnika radi beleženja rezervacija i pravilnog upravljanja letom. Avio-kompaniji su potrebni podaci o brojevima sedišta putnika, posebnim telesnim ograničenjima, kao što su potrebe osoba u invalidskim kolicima, kao i posebnim prehrambenim zahtevima, kao što su košer ili halal hrana. Ako se od avio-kompanije zatraži prenos tih podataka, koji se nalaze u evidenciji imena putnika, organima nadležnim za imigraciju na odredišnom aerodromu, ti podaci se zatim upotrebljavaju u svrhu kontrole imigracije koja se razlikuje od početne svrhe prikupljanja podataka. Stoga je za prenos tih podataka organu nadležnom za imigraciju potrebna nova i zasebna pravna osnova.

Pri razmatranju oblasti primene i ograničenja određene svrhe, modernizovana Konvencija br. 108 i Opšta uredba o zaštiti podataka zasnivaju se na načelu usklađenosti: upotreba podataka u spojive svrhe dopuštena je na osnovu prvobitne pravne osnove. Stoga se dalja obrada podataka ne može vršiti na način koji je neočekivan ili neprimeren za ispitanika ili kojem se on može protiviti[289]. Da bi se ocenilo da li može dalja obrada da se smatra usklađenom, rukovalac podacima treba da uzme u obzir sledeće (između ostalog):

- „svaku vezu između te svrhe i svrhe planiranog nastavka obrade,
- kontekst u kome su prikupljeni lični podaci, posebno opravdana očekivanja ispitanika koja se zasnivaju na njihovom odnosu sa rukovaocem podacima u pogledu dalje upotrebe podataka,

289 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 49.

- prirodu ličnih podataka,
- posledice planiranog nastavka obrade za ispitanike i
- postojanje primerenih zaštitnih mera u izvornoj i planiranoj daljoj obradi[290].“ To se na primer može postići šifrovanjem ili pseudonimizacijom.

Primer: Kompanija Sunshine dolazi do podataka o kupcima tokom upravljanja odnosima s kupcima (CRM). Zatim te podatke prenosi kompaniji Moonlight koja se bavi neposrednim marketingom, a koja te podatke želi da iskoristi kao pomoć u marketinškim kampanjama trećih kompanija. Prenos podataka koji vrši kompanija Sunshine radi marketinga drugih kompanija predstavlja naknadnu upotrebu podataka u novu svrhu, koja nije usklađena sa CRM-om, prvobitnom svrhom prikupljanja podataka o kupcima kompanije Sunshine. Stoga prenos podataka kompaniji Moonlight iziskuje sopstvenu pravnu osnovu.

Za razliku od toga, upotreba podataka iz CRM-a u svrhe sopstvenog marketinga kompanije Sunshine, odnosno slanje marketinških poruka sopstvenim kupcima za sopstvene proizvode, generalno je prihvaćena kao spojiva svrha.

U Opštoj uredbi o zaštiti podataka i modernizovanoj Konvenciji br. 108 utvrđuje se da se „dalja obrada u svrhe arhiviranja u javnom interesu, u svrhe naučnog ili istorijskog istraživanja ili u statističke svrhe“ *a priori* smatra usklađenom s prvobitnom svrhom[291]. Međutim, prilikom dalje obrade ličnih podataka moraju se uspostaviti odgovarajuće zaštitne mere poput anonimizacije, šifrovanja ili pseudonimizacije podataka kao i ograničenja pristupa podacima[292]. U Opštoj uredbi o zaštiti podataka dodaje se sledeće: „Ako je ispitanik dao pristanak ili se obrada zasniva na pravu Unije ili pravu države članice koje čini potrebnu i srazmernu meru u demokratskom društvu posebno za zaštitu važnih ciljeva od opšteg javnog interesa, rukovaocu podacima trebalo bi dozvoliti dalju obradu ličnih podataka nezavisno od spojivosti

290 Opšta uredba o zaštiti podataka, uvodna izjava 50. i član 6. stav 4.; Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 49.

291 Opšta uredba o zaštiti podataka, član 5. stav 1. tačka (b); modernizovana Konvencija br. 108, član 5. stav 4. tačka (b). Primer nacionalnih odredbi je austrijski Zakon o zaštiti podataka (Datenschutzgesetz), Savezni službeni list I br. 165/1999, stav 46.

292 Opšta uredba o zaštiti podataka, član 6. stav 4.; modernizovana Konvencija br. 108, član 5. stav 4. tačka (b); Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 50.

svrha"[293]. Prilikom dalje obrade ispitanik stoga treba da bude obavešten o svrhama i svojim pravima, poput prava na prigovor[294].

Primer: Kompanija Sunshine prikupila je i sačuvala podatke o upravljanju odnosima s kupcima (CRM) o svojim kupcima. Kompanija Sunshine sme dalje da upotrebljava te podatke radi statističke analize ponašanja svojih kupaca prilikom kupovine jer je statistika spojiva svrha. Nije potrebna dodatna pravna osnova, kao što je pristanak ispitanika. Međutim, za dalju obradu ličnih podataka u statističke svrhe kompanija Sunshine mora da uspostavi odgovarajuće zaštitne mere za prava i slobode ispitanika. Tehničke i organizacione mere koje kompanija Sunshine mora da sprovede mogu uključivati pseudonimizaciju.

3.3. Načelo smanjenja količine podataka

Ključne tačke

- Obrada podataka mora biti ograničena na ono što je nužno za ispunjavanje legitimne svrhe.
- Obrada ličnih podataka treba da se vrši samo kada svrha obrade ne može razumno da se postigne drugim sredstvima.
- Obradom podataka ne sme se nesrazmerno mešati u interese, prava i slobode o kojima je reč.

Obrađuju se samo podaci koji su „primereni, relevantni i nepreopsežni u odnosu na svrhu njihovog prikupljanja i/ili dalje obrade"[295]. Kategorije podataka odabranih za obradu moraju biti nužne za postizanje navedenog opšteg cilja postupka obrade, a rukovalac podacima treba strogo da ograniči prikupljanje podataka na one informacije koje su neposredno važne za konkretnu svrhu obrade.

293 Opšta uredba o zaštiti podataka, uvodna izjava 50.

294 *Ibid.*

295 Modernizovana Konvencija br. 108, član 5. stav 4. tačka (c); Opšta uredba o zaštiti podataka, član 5. stav 1. tačka (c).

Primer: U predmetu *Digital Rights Ireland*[296] SPEU je razmatrao valjanost Direktive o zadržavanju podataka, kojom su nastojale da se usklade domaće odredbe o zadržavanju ličnih podataka koji se generišu ili obrađuju javno dostupnim elektronskim komunikacionim uslugama ili mrežama radi njihovog mogućeg prenosa nadležnim organima za borbu protiv teških zločina poput organizovanog kriminala i terorizma. Bez obzira na činjenicu da se to smatralo svrhom kojom se zaista ostvaruje cilj od opšteg interesa, uopšteni način na koji je Direktiva obuhvatala „svaku osobu i sva sredstva elektronske komunikacije kao i sve podatke o prometu bez ikakvog razlikovanja, ograničenja ili izuzetka s obzirom na cilj borbe protiv teških krivičnih dela" smatrao se problematičnim[297].

Zatim, upotrebom posebne tehnologije za povećanje privatnosti ponekad je moguće sasvim izbeći upotrebu ličnih podataka ili upotrebiti mere za smanjenje mogućnosti pripisivanja podataka ispitaniku (na primer, pseudonimizacijom), čime se postiže povoljno rešenje za privatnost. To je naročito prikladno u opsežnijim sistemima obrade.

Primer: Gradsko Veće redovnim korisnicima sistema javnog gradskog prevoza nudi čip-karticu uz određenu naknadu. Na površini kartice navedeno je ime korisnika u pisanom obliku, a u čipu u elektronskom obliku. Pri svakoj vožnji autobusom ili tramvajem čip-kartica se postavlja ispred ugrađenih uređaja za očitavanje, na primer, u autobusima i tramvajima. Podaci koje uređaj očita elektronski se proveravaju u bazi podataka s imenima ljudi koji su kupili putnu kartu.

Taj sistem nije usklađen s načelom smanjenja količine podataka na optimalan način: provera da li osoba sme da upotrebljava sredstva javnog prevoza mogla bi se izvršiti bez poređenja ličnih podataka sa čip-kartice s onima iz baze podataka. Bilo bi dovoljno, na primer, imati posebnu elektronsku sliku, kao što je bar-kod, u čipu kartice kojim bi se, kad se kartica postavi ispred uređaja za čitanje, potvrdila valjanost kartice. Takvim sistemom se ne bi beležilo ko je i kada upotrebljavao određeno prevozno sredstvo. To bi bilo optimalno rešenje u smislu načela smanjenja količine podataka jer iz tog načela proizlazi obaveza smanjenja prikupljanja podataka.

296 SPEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr.* i *Kärntner Landesregierung i dr.* [VV], 8. aprila 2014.

297 *Ibid.*, st. 44 i 57.

Član 5. stav 1. modernizovane Konvencije br. 108 sadrži zahtev srazmernosti za obradu ličnih podataka u vezi sa legitimnom svrhom koja treba da se postigne. Mora se uspostaviti pravična ravnoteža među svim predmetnim interesima, u svim fazama obrade. To znači da „[l]ični podaci koji su dovoljni i relevantni, ali koji bi uključivali neproporcionalno mešanje u predmetna osnovna prava i slobode treba da se smatraju preopsežnima"[298].

3.4. Načelo tačnosti podataka

Ključne tačke

- Načelo tačnosti podataka mora sprovoditi rukovalac podacima u svim postupcima obrade.
- Netačni podaci moraju se izbrisati ili ispraviti bez odlaganja.
- Podaci će možda morati da se redovno proveravaju i ažuriraju da bi se obezbedila tačnost.

Rukovalac podacima koji raspolaže ličnim podacima ne sme te podatke da upotrebljava bez preduzimanja mera kojima se može relativno jasno obezbediti da podaci budu tačni i ažurni[299].

Obavezu obezbeđivanja tačnosti podataka treba posmatrati u kontekstu svrhe obrade podataka.

Primer: U predmetu *Rijkeboer*[300] SPEU je razmatrao zahtev državljanina Holandije za prijem informacija od lokalnih gradskih vlasti u Amsterdamu o identitetu osoba kojima su lokalne vlasti davale zapise o njemu tokom prethodne dve godine, kao i o sadržaju otkrivenih podataka. SPEU je utvrdio da „pravo na privatnost znači da ispitanik može da bude siguran da se njegovi

298 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, član 52.; Opšta uredba o zaštiti podataka, član 5. stav 1. tačka (c).

299 Opšta uredba o zaštiti podataka, član 5. stav 1. tačka (d); modernizovana Konvencija br. 108, član 5. stav 4. tačka (d).

300 SPEU, C-553/07, *College van burgemeester en wethouders van Rotterdam protiv M. E. E. Rijkeboer*, 7. maja 2009.

lični podaci obrađuju na pravilan i zakonit način, odnosno da su osnovni podaci o njemu tačni i da se otkrivaju ovlašćenim primaocima". SPEU je zatim uputio na preambulu Direktive o zaštiti podataka, u kojoj se navodi da ispitanici moraju uživati pravo pristupa svojim ličnim podacima kako bi mogli da provere njihovu tačnost[301].

Takođe mogu postojati slučajevi u kojima je ažuriranje sačuvanih podataka zakonom zabranjeno, jer je osnovna svrha čuvanja podataka dokumentovanje događaja kao istorijskog zapisa.

Primer: Medicinska dokumentacija o operaciji ne sme se izmeniti, odnosno „ažurirati", čak i ako se nalazi spomenuti u njoj kasnije pokažu pogrešnima. U takvim okolnostima u dokumentaciju se smeju dodati samo napomene koje moraju biti jasno označene kao naknadno dodati unosi.

S druge strane, postoje situacije u kojima su redovna provera tačnosti podataka i njihovo ažuriranje apsolutno nužni zbog moguće štete koju može pretrpeti ispitanik ako podaci ostanu netačni.

Primer: Ako osoba želi da sklopi ugovor o kreditu sa bankovnom institucijom, banka obično proverava kreditnu sposobnost mogućeg klijenta. Za to postoje posebne baze podataka u kojima su sadržani podaci o kreditnoj istoriji privatnih lica. Ako su u takvoj bazi podataka navedeni netačni ili zastareli podaci o ličnosti, ona može pretrpeti negativne posledice. Rukovaoci podacima takvih baza podataka stoga moraju posebno da se potrude da poštuju načelo tačnosti.

3.5. Načelo ograničenja čuvanja

Ključne tačke

- Načelo ograničenja čuvanja znači da se lični podaci moraju izbrisati ili anonimizovati čim prestanu da budu potrebni za svrhe za koje su prikupljeni.

301 Nekadašnja uvodna izjava 41, preambula Direktive 95/46/EZ.

Članom 5. stav 1. tačka (e) OUZP-a i članom 5. stav 4. tačkom (e) modernizovane Konvencije br. 108 propisuje se da lični podaci moraju biti „čuvani u obliku koji omogućava identifikaciju ispitanikâ samo onoliko dugo koliko je potrebno u svrhe radi kojih se lični podaci obrađuju". Dakle, podaci se moraju izbrisati ili anonimizovati nakon ispunjavanja tih svrha. U tu svrhu, „rukovalac podacima bi trebalo da odredi rok za brisanje ili periodično preispitivanje" kako bi se obezbedilo da se podaci ne čuvaju duže nego što je nužno[302].

U predmetu *S. i Marper* ESLJP je zaključio da ključna načela odgovarajućih instrumenata Saveta Evrope, kao i pravo i praksa drugih ugovornih strana, nalažu da zadržavanje podataka bude srazmernono u odnosu na svrhu prikupljanja i vremenski ograničeno, naročito u policijskom sektoru[303].

Primer: U predmetu *S. i Marper*[304] ESLJP je presudio da zadržavanje otisaka prstiju, uzoraka ćelija i profila DNK-a dvojice podnosilaca predstavki na neodređeni period nije srazmerno niti nužno u demokratskom društvu, budući da je krivični postupak protiv obojice podnosilaca predstavki prekinut oslobođenjem, odnosno obustavom postupka.

Vremensko ograničenje za čuvanje ličnih podataka odnosi se samo na podatke koji se čuvaju u obliku koji omogućava identifikaciju ispitanika. Stoga bi se zakonito čuvanje podataka koji više nisu potrebni moglo postići anonimizacijom podataka.

Arhiviranje podataka zbog javnog interesa, u naučne ili istorijske svrhe ili upotrebu u statističkim analizama, može se vršiti na duže periode, pod uslovom da se takvi podaci upotrebljavaju isključivo u navedene svrhe[305]. Za trajno čuvanje i upotrebu ličnih podataka nužno je izvršiti odgovarajuće tehničke i organizacione mere kako bi se zaštitila prava i slobode ispitanika.

Modernizovanom Konvencijom br. 108 dopuštaju se i izuzeci od načela ograničenja čuvanja pod uslovom da su oni propisani zakonom, da se njima poštuje suština osnovnih prava i sloboda i da su oni nužni i proporcionalni za ostvarenje ograni-

302 Opšta uredba o zaštiti podataka, uvodna izjava 39.

303 ESLJP, *S. i Marper protiv Ujedinjenog Kraljevstva* [VV], br. 30562/04 i 30566/04, 4. decembra 2008; na primer, videti i: ESLJP, *M. M. protiv Ujedinjenog Kraljevstva*, br. 24029/07, 13. novembra 2012.

304 ESLJP, *S. i Marper protiv Ujedinjenog Kraljevstva* [VV], br. 30562/04 i 30566/04, 4. decembra 2008.

305 Opšta uredba o zaštiti podataka, član 5. stav 1. tačka (e); modernizovana Konvencija br. 108, član 5. stav 4. tačka (b) i član 11. stav 2.

čenog broja legitimnih ciljeva[306]. Oni, između ostalog, uključuju zaštitu nacionalne bezbednosti, istragu i gonjenje krivičnih dela, izvršavanje krivičnih sankcija, zaštitu ispitanika kao i zaštitu prava i osnovnih sloboda drugih.

Primer: U predmetu *Digital Rights Ireland*[307] SPEU je preispitao valjanost Direktive o zadržavanju podataka kojom se nastojalo da se usklade domaće odredbe o zadržavanju ličnih podataka koji se generišu ili obrađuju javno dostupnim elektronskim komunikacionim uslugama ili mrežama radi borbe protiv teških zločina poput organizovanog kriminala i terorizma. Direktivom o zadržavanju podataka propisan je period zadržavanja podataka „koji nije kraći od šest meseci, a da se pritom ne navodi nikakvo razlikovanje između kategorija podataka predviđenih u članu 5. te direktive s obzirom na njihovu eventualnu korist za cilj koji se sledi ili s obzirom na lica na koja se odnosi"[308]. SPEU je takođe izneo problem izostanka objektivnih kriterijuma u Direktivi o zadržavanju podataka na osnovu kojih se određuje tačan period zadržavanja podataka – koji može da varira od najmanje šest meseci do najviše 24 meseca – kako bi se obezbedilo da razdoblje bude ograničeno na ono što je strogo nužno[309].

3.6. Načelo bezbednosti podataka

Ključne tačke

- Bezbednost i poverljivost ličnih podataka su ključne za sprečavanje štetnih posledica po ispitanika.
- Bezbednosne mere mogu biti tehničke i/ili organizacione prirode.
- Pseudonimizacija je postupak kojim se mogu zaštititi lični podaci.
- Primerenost bezbednosnih mera mora se odrediti za svaki pojedinačni slučaj i redovno se preispitivati.

306 Modernizovana Konvencija br. 108, član 11. stav 1.; Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, st. od 91 do 98.

307 SPEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr.* i *Kärntner Landesregierung i dr.* [VV], 8. aprila 2014.

308 *Ibid.*, stav 63.

309 *Ibid.*, stav 64.

Prema načelu bezbednosti podataka, potrebno je sprovesti odgovarajuće tehničke ili organizacione mere prilikom obrade ličnih podataka kako bi se podaci zaštitili od nehotičnog, neovlašćenog ili nezakonitog pristupa, upotrebe, izmene, otkrivanja, gubitka, uništenja ili oštećenja[310]. U OUZP-u se navodi da rukovalac podacima i obrađivač podataka prilikom sprovođenja takvih mera treba da uzmu u obzir „najnovija dostignuća, troškove sprovođenja i prirodu, opseg, kontekst i svrhe obrade, kao i rizik različitih nivoa verovatnoće i ozbiljnosti za prava i slobode pojedinaca"[311]. Zavisno od okolnosti pojedinačnog slučaja, odgovarajuće tehničke i organizacione mere mogu uključivati, na primer, pseudonimizaciju i enkripciju ličnih podataka i/ili redovno testiranje i procenjivanje delotvornosti mera za obezbeđivanje sigurnosti obrade podataka[312].

Kao što je objašnjeno u delu 2.1.1, pseudonimizacija podataka znači zamenu atributa ličnih podataka – koji omogućavaju identifikaciju ispitanika – pseudonimom i čuvanje tih atributa na odvojenom mestu, zaštićene tehničkim ili organizacionim merama. Postupak pseudonimizacije ne sme se zameniti postupkom anonimizacije, u kojem se uklanjanju sve veze sa identitetom osobe.

Primer: Rečenica „Čarls Spenser, rođen 3. aprila 1967. godine, otac je četvoro dece, dvaju dečaka i dveju devojčica", može se, na primer, pseudonimizovati na sledeći način:

„Č. S. 1967. otac je četvoro dece, dvaju dečaka i dveju devojčica" ili

„324 otac je četvoro dece, dvaju dečaka i dveju devojčica" ili

„YESz320l otac je četvoro dece, dvaju dečaka i dveju devojčica".

Korisnici koji pristupe pseudonimizovanim podacima obično neće moći da identifikuju „Čarlsa Spensera, rođenog 3. aprila 1967." na osnovu pseudonima „324" ili „YESz3201". Stoga će takvi podaci verovatno češće zaštićeni od zloupotrebe.

310 Opšta uredba o zaštiti podataka, uvodna izjava 39 i član 5. stav 1. tačka (f); modernizovana Konvencija br. 108, član 7.

311 Opšta uredba o zaštiti podataka, član 32. stav 1.

312 *Ibid*.

Međutim, prvi navedeni primer je manje bezbedan. Ako se rečenica „Č. S. 1967. otac je četvoro dece, dvaju dečaka i dveju devojčica" koristi u malom selu u kojem Čarls Spenser živi, mogao bi lako da se prepozna. Metoda pseudonimizacije može uticati na efikasnost zaštite podataka.

Lični podaci sa šifrovanim ili zasebno čuvanim atributima upotrebljavaju se u mnogim kontekstima radi očuvanja tajnosti ličnog identiteta. To je naročito korisno kada rukovaoci podacima moraju biti sigurni da se bave istim ispitanicima, tj. licima čiji se podaci obrađuju, ali ne zahtevaju, ili ne bi smeli da saznaju, stvarni identitet tih osoba. To se događa kada, na primer, istraživač istražuje tok bolesti pacijenata čiji je identitet poznat samo bolnici u kojoj se pacijenti leče i koja istraživaču dostavlja pseudonimizovane istorije slučajeva. Pseudonimizacija je, dakle, snažna karika u lancu tehnologije za zaštitu privatnosti. Ona može biti važan elemenat u sprovođenju tehničke zaštite privatnosti. To znači da je zaštita podataka ugrađena u tkivo sistema obrade podataka.

U članu 25. OUZP-a, u kojem se obrađuje tehnička zaštita podataka, izričito se navodi pseudonimizacija kao primer odgovarajuće tehničke i organizacione mere koju rukovaoci podacima treba da sprovedu radi omogućavanja primene načela zaštite podataka i uključenja potrebnih zaštitnih mera. Time će rukovaoci podacima ispuniti zahteve iz Uredbe i zaštititi prava ispitanika prilikom obrade njihovih ličnih podataka.

Poštovanje odobrenog kodeksa ponašanja ili odobrenog mehanizma sertifikovanja može se iskoristiti za dokazivanje usklađenosti sa zahtevom bezbednosti obrade[313]. Savet Evrope u svom Mišljenju o implikacijama obrade evidencije imena putnika za zaštitu podataka navodi druge primere odgovarajućih bezbednosnih mera za zaštitu ličnih podataka u sistemima evidencije imena putnika. One uključuju čuvanje podataka u bezbednom fizičkom okruženju, ograničenje pristupa putem različitih nivoa prijave i zaštitu prenosa podataka snažnom kriptografijom[314].

Primer: Internet stranice društvenih mreža i pružaoci usluga elektronske pošte omogućavaju korisnicima postavljanje dodatnog nivoa bezbednosti podataka u uslugama koje pružaju zahvaljujući uvođenju dvostruke provere autentičnosti.

313 *Ibid.*, član 32. stav 3.

314 Savet Evrope, Odbor za Konvenciju br. 108, *Opinion on the Data protection implications of the processing of Passenger Name Records* (Mišljenje o implikacijama obrade evidencija imena putnika za zaštitu podataka), T-PD(2016)18rev, 19. avgusta 2016, str. 9.

Uz unos lične lozinke, korisnici moraju obaviti drugu prijavu da bi pristupili svom korisničkom računu. To može uključivati, na primer, unos bezbednosnog koda koji se šalje na broj mobilnog telefona povezan sa korisničkim računom. Na taj način provera u dva koraka obezbeđuje bolju zaštitu ličnih podataka od neovlašćenog pristupa hakera korisničkim računima.

U Izveštaju s objašnjenjima o modernizovanoj Konvenciji br. 108 daju se dodatni primeri odgovarajućih zaštitnih mera, kao što je primena obaveze čuvanja poslovne tajne ili usvajanje primerenih tehničkih sigurnosnih mera kao što je šifrovanje podataka[315]. Prilikom uspostavljanja pojedinih sigurnosnih mera, rukovalac podacima ili, kada je to primenjivo, obrađivač podataka, treba da uzme u obzir nekoliko elemenata, kao što su priroda i količina ličnih podataka koji se obrađuju, moguće štetne posledice po ispitanike i potreba za ograničenim pristupom podacima[316]. Prilikom sprovođenja odgovarajućih sigurnosnih mera moraju se razmotriti najsavremenije postojeće metode i tehnike bezbednosti podataka u oblasti obrade podataka. Trošak takvih mera mora biti srazmeran ozbiljnosti i verovatnoći mogućih rizika. Neophodno je redovno preispitivanje sigurnosnih mera kako bi po potrebi mogle da se ažuriraju[317].

U slučajevima povrede ličnih podataka, i modernizovanom Konvencijom br. 108 i OUZP-om zahteva se da rukovalac podacima bez nepotrebnog odlaganja obavesti nadležni nadzorni organ o povredi, kao i o rizicima za prava i slobode pojedinaca[318]. Slična obaveza obaveštavanja ispitanika primenjuje se i kada je verovatno da će povreda ličnih podataka prouzrokovati visok rizik za njegova prava i slobode[319]. Ispitanici se o takvim povredama moraju obavestiti upotrebom jasnog i jednostavnog jezika[320]. Ako obrađivač podataka sazna za povredu ličnih podataka, odmah mora obavestiti rukovaoca podacima[321]. U određenim situacijama mogu se primenjivati izuzeci od obaveze obaveštavanja. Na primer, rukovalac podacima ne mora obavestiti nadzorno telo „ako nije verovatno da će povreda ličnih podataka prouzro-

315 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 56.

316 *Ibid.*, stav 62.

317 *Ibid.*, stav 63.

318 Modernizovana Konvencija br. 108, član 7. stav 2.; Opšta uredba o zaštiti podataka, član 33. stav 1.

319 Modernizovana Konvencija br. 108, član 7. stav 2.; Opšta uredba o zaštiti podataka, član 34. stav 1.

320 Opšta uredba o zaštiti podataka, član 34. stav 2.

321 *Ibid.*, član 33. stav 1.

kovati rizik za prava i slobode pojedinaca"[322]. Isto tako, nije potrebno obavestiti ispitanika kada primenjene sigurnosne mere učine podatke nerazumljivima neovlašćenim osobama ili kada zbog naknadnih mera više nije verovatno da će doći do visokog rizika[323]. Ako bi obaveštavanje ispitanika o povredi ličnih podataka iziskivalo nesrazmeran napor rukovaoca podacima, javnim obaveštavanjem ili sličnom merom može se obezbediti da se „ispitanici obaveštavaju na podjednako delotvoran način"[324].

3.7. Načelo odgovornosti

Ključne tačke

- Prema načelu odgovornosti, rukovaoci podacima i obrađivači podataka moraju tokom svojih aktivnosti obrade aktivno i neprekidno da sprovode mere za unapređenje i obezbeđenje zaštite podataka.
- Rukovaoci podacima i obrađivači podataka odgovorni su za usklađenost svojih postupaka obrade sa pravom zaštite podataka i svojim pojedinačnim obavezama.
- Rukovaoci podacima moraju da budu u mogućnosti u svakom trenutku da dokažu usklađenost s odredbama o zaštiti podataka ispitanicima, javnosti i nadzornim organima. Obrađivači podataka, takođe, moraju da se pridržavaju određenih obaveza koje su strogo povezane s odgovornošću (poput vođenja evidencije o postupcima obrade i imenovanja službenika za zaštitu podataka).

U OUZP-u i modernizovanoj Konvenciji br. 108 utvrđeno je da je rukovalac podacima odgovoran za usklađenost s načelima obrade ličnih podataka opisanima u ovom poglavlju i da to mora biti u mogućnosti da dokaže[325]. U tu svrhu rukovalac podacima mora da sprovede odgovarajuće tehničke i organizacione mere[326]. Iako se načelo odgovornosti iz člana 5. stav 2. OUZP-a odnosi samo na rukovaoce podacima, odgovornost se očekuje i od obrađivača podataka, budući da oni moraju da se pridržavaju nekolikih obaveza i da su usko povezani s odgovornošću.

322 *Ibid*.

323 *Ibid*., član 34. stav 3. tačke (a) i (b).

324 *Ibid*., član 34. stav 3. tačka (c).

325 *Ibid*., član 5. stav 2.; modernizovana Konvencija br. 108, član 10. stav 1.

326 Opšta uredba o zaštiti podataka, član 24.

Propisima o zaštiti podataka EU i Saveta Evrope takođe se propisuje da je rukovalac podacima odgovoran za usklađenost sa načelima zaštite podataka opisanima u delovima od 3.1. do 3.6. i da bi trebalo da bude u mogućnosti da to obezbedi[327]. Radna grupa iz člana 29. ističe da bi se „vrsta postupaka i mehanizama razlikovala prema rizicima koje predstavljaju obrada i priroda podataka"[328].

Rukovaoci podacima mogu da olakšaju usklađenost s ovim zahtevom na različite načine, uključujući sledeće:

- vođenje evidencije aktivnosti obrade i njeno davanje na uvid nadzornom organu na zahtev[329],
- u određenim situacijama, imenovanje službenika za zaštitu podataka koji će biti uključen u sva pitanja u pogledu zaštite ličnih podataka[330],
- sprovođenje procene efekta zaštite podataka za one vrste obrade za koje je verovatno da će prouzrokovati visok rizik za prava i slobode pojedinaca[331],
- obezbeđenje tehničke i integrisane zaštite podataka[332],
- sprovođenje modaliteta i postupaka za ostvarivanje prava ispitanika[333],
- pridržavanje odobrenih kodeksa ponašanja ili mehanizama sertifikovanja[334].

Iako se načelo odgovornosti iz člana 5. stav 2. OUZP-a ne odnosi izričito na obrađivače podataka, određene odredbe u vezi sa odgovornošću takođe sadrže obaveze za njih, poput vođenja evidencije o aktivnostima obrade i imenovanja službenika za zaštitu podataka za sve aktivnosti obrade za koje je on potreban[335]. Obrađivači podataka takođe moraju da obezbede da budu sprovedene sve mere potrebne za

327 *Ibid.*, član 5. stav 2.; modernizovana Konvencija br. 108, član 10. stav 1.

328 Radna grupa iz člana 29., *Opinion 3/2010 on the principle of accountability* (Mišljenje 3/2010 o načelu odgovornosti), WP 173, Bruxelles, 13. jula 2010., stav 12.

329 Opšta uredba o zaštiti podataka, član 30.

330 *Ibid.*, čl. od 37 do 39.

331 *Ibid.*, član 35; modernizovana Konvencija br. 108, član 10. stav 2.

332 Opšta uredba o zaštiti podataka, član 25.; modernizovana Konvencija br. 108, član 10. stavovi 2 i 3.

333 *Ibid.*, član 12. i član 24.

334 *Ibid.*, član 40. i član 42.

335 *Ibid.*, član 5. stav 2., čl. 30 i 37.

sigurnost podataka[336]. U pravno obavezujućem ugovoru između rukovaoca podacima i obrađivača podataka mora se utvrditi da obrađivač podataka pomaže rukovaocu podacima u vezi s određenim zahtevima usklađenosti, na primer prilikom obavljanja procene efekta zaštite podataka ili obaveštavanja rukovaoca podacima o svakoj povredi ličnih podataka čim za nju sazna[337].

Godine 2013. Organizacija za ekonomsku saradnju i razvoj (OECD) donela je smernice o privatnosti kojima se naglašava da rukovaoci podacima imaju važnu ulogu u obezbeđivanju funkcionisanja zaštite podataka u praksi. U smernicama se načelo odgovornosti opisuje na sledeći način: „rukovalac podacima treba da bude odgovoran za usklađenost sa merama kojima se sprovode spomenuta [materijalna] načela"[338].

Primer: Primer iz zakonodavstva kojim se naglašava načelo odgovornosti jeste izmena i dopuna[339] Direktive o privatnosti i elektronskim komunikacijama 2002/58/EZ iz 2009. Prema članu 4. u njegovom izmenjenom obliku, direktivom se nameće obaveza da mere „obezbeđuju sprovođenje bezbednosne politike s obzirom na obradu ličnih podataka". Dakle, u pogledu odredbi o bezbednosti iz te direktive, zakonodavac je odlučio da je potrebno izričito usloviti postojanje i sprovođenje bezbednosne politike.

336 *Ibid*., član 28. stav 3. tačka (c).

337 *Ibid*., član 28. stav 3. tačka (d).

338 OECD (2013.), Smernice kojima se uređuju zaštita privatnosti i prekogranični prenosi ličnih podataka, član 14.

339 Direktiva 2009/136/EZ Evropskog parlamenta i Saveta od 25. novembra 2009. o izmeni Direktive 2002/22/EZ o univerzalnim uslugama i pravima korisnika s obzirom na elektronske komunikacione mreže i usluge, Direktive 2002/58/EZ o obradi ličnih podataka i zaštiti privatnosti u sektoru elektronskih komunikacija i Uredbe (EZ) br. 2006/2004 o saradnji između nacionalnih tela odgovornih za sprovođenje zakona o zaštiti potrošača, SL 2009 L 337, str. 11.

Prema mišljenju Radne grupe iz člana 29.[340], suština odgovornosti je obaveza rukovaoca podacima da:

- uvede mere kojima bi se u uobičajenim okolnostima garantovalo poštovanje pravila o zaštiti podataka u kontekstu postupaka obrade i da

- ima spremnu dokumentaciju kojom se ispitanicima i nadzornim organima može dokazati koje su potrebne mere preduzete kako bi se obezbedila usklađenost s propisima o zaštiti podataka.

Prema načelu odgovornosti od rukovaoca podacima se stoga zahteva sposobnost aktivnog dokazivanja usklađenosti umesto čekanja da ispitanici ili nadzorni organi ukažu na nedostatke.

340 Radna grupa iz člana 29., Opinion 3/2010 on the principle of accountability, WP 173, Bruxelles, 13. jula 2010.

4

Odredbe evropskog prava zaštite podataka

EU	Obuhvaćena pitanja	Savet Evrope
Propisi o zakonitoj obradi podataka		
Opšta uredba o zaštiti podataka, član 6. stav 1. tačka (a) SPEU, C-543/09, *Deutsche Telekom AG protiv Bundesrepublik Deutschland*, 2011. SPEU, C-536/15, *Tele2 (Netherlands) BV i dr. protiv Autoriteit Consument en Markt (ACM)*, 2017.	Pristanak	Profiling Recommendation (Preporuka o izradi profila), član 3.4. tačka (b) i član 3.6. Modernizovana Konvencija br. 108, član 5. stav 2.
Opšta uredba o zaštiti podataka, član 6. stav 1. tačka (b)	(Pred)ugovorni odnos	Preporuka o izradi profila, član 3.4. tačka (b)
Opšta uredba o zaštiti podataka, član 6. stav 1.tačka (c)	Pravne dužnosti rukovaoca podacima	Preporuka o izradi profila, član 3.4. tačka (a)
Opšta uredba o zaštiti podataka, član 6. stav 1. tačka (d)	Vitalni interesi ispitanika	Preporuka o izradi profila, član 3.4. tačka (b)
Opšta uredba o zaštiti podataka, član 6. stav 1. tačka (e) SPEU, C-524/06, *Huber protiv Bundesrepublik Deutschland* [VV], 2008.	Javni interes i izvršavanje javnog ovlašćenja	Preporuka o izradi profila, član 3.4. tačka (b)

EU	Obuhvaćena pitanja	Savet Evrope
Opšta uredba o zaštiti podataka, član 6. stav 1. tačka (f) SPEU, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde protiv Rīgas pašvaldības SIA „Rīgas satiksme"*, 2017. SPEU, spojeni predmeti C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) protiv Administración del Estado*, 2011.	Legitimni interesi drugih	Preporuka o izradi profila, član 3.4. tačka (b) ESLJP, *Y protiv Turske*, br. 648/10, 2015.
Opšta uredba o zaštiti podataka, član 6. stav 4.	Izuzeće od ograničenja svrhe: dalja obrada u druge svrhe	Modernizovana Konvencija br. 108, član 5. stav 4. tačka (b)
Propisi o zakonitoj obradi osetljivih podataka		
Opšta uredba o zaštiti podataka, član 9. stav 1.	Opšta zabrana obrade	Modernizovana Konvencija br. 108, član 6.
Opšta uredba o zaštiti podataka, član 9. stav 2.	Izuzeća od opšte zabrane	Modernizovana Konvencija br. 108, član 6.
Propisi o bezbednoj obradi		
Opšta uredba o zaštiti podataka, član 32.	Obaveza osiguravanja bezbedne obrade	Modernizovana Konvencija br. 108, član 7. stav 1. ESLJP, *I protiv Finske*, br. 20511/03, 2008.
Opšta uredba o zaštiti podataka, član 28. i član 32. stav 1. tačka (b)	Obaveza poverljivosti	Modernizovana Konvencija br. 108, član 7. stav 1.
Opšta uredba o zaštiti podataka, član 34. Direktiva o privatnosti i elektronskim komunikacijama, član 4. stav 2.	Obaveštavanje u slučaju povrede podataka	Modernizovana Konvencija br. 108, član 7. stav 2.
Propisi o odgovornosti i unapređenju usklađenosti		
Opšta uredba o zaštiti podataka, članovi 12., 13. i 14.	Transparentnost uopšte	Modernizovana Konvencija br. 108, član 8.
Opšta uredba o zaštiti podataka, članovi 37., 38. i 39.	Službenici za zaštitu podataka	Modernizovana Konvencija br. 108, član 10. stav 1.
Opšta uredba o zaštiti podataka, član 30.	Evidencija aktivnosti obrade	

EU	Obuhvaćena pitanja	Savet Evrope
Opšta uredba o zaštiti podataka, članovi 35. i 36.	Procena efekta i prethodno savetovanje	Modernizovana Konvencija br. 108, član 10. stav 2.
Opšta uredba o zaštiti podataka, članovi 33. i 34.	Obaveštavanje u slučaju povrede podataka	Modernizovana Konvencija br. 108, član 7. stav 2.
Opšta uredba o zaštiti podataka, članovi 40. i 41.	Kodeksi ponašanja	
Opšta uredba o zaštiti podataka, članovi 42. i 43.	Sertifikovanje	
Tehnička i integrisana zaštita podataka		
Opšta uredba o zaštiti podataka, član 25. stav 1.	Tehnička zaštita podataka	Modernizovana Konvencija br. 108, član 10. stav 2.
Opšta uredba o zaštiti podataka, član 25. stav 2.	Integrisana zaštita podataka	Modernizovana Konvencija br. 108, član 10. stav 3.

Načela su nužno uopštene prirode. Kad se primenjuju na konkretne situacije, postoji određena sloboda tumačenja i izbor sredstava. **Prema pravu Saveta Evrope**, ugovornicama modernizovane Konvencije br. 108 prepušta se da pojasne tu slobodu tumačenja u svojim domaćim zakonodavstvima. U **pravu Evropske unije** situacija je drugačija: za uspostavu zaštite podataka na unutrašnjem tržištu smatralo se da su nužna detaljnija pravila na nivou EU radi usklađivanja nivoa zaštite podataka u okviru domaćih zakonodavstava država članica. Opštom uredbom o zaštiti podataka uspostavlja se sloj detaljnih pravila prema načelima utvrđenim u njenom članu 5., koja su direktno primenjiva unutar domaćeg pravnog poretka. Stoga se sledeće napomene o detaljnim pravilima zaštite podataka na evropskom nivou pretežno odnose na pravo EU.

4.1. Propisi o zakonitoj obradi

Ključne tačke

- Lični podaci se mogu zakonito obraditi ako ispunjavaju neki od sledećih kriterijuma:
  - obrada se zasniva na pristanku ispitanika,
  - obrada ličnih podataka uslovljava se ugovornim odnosom,

  - obrada je nužna za ispunjavanje zakonskih obaveza rukovaoca podacima,
  - obrada podataka nužna je zbog vitalnih interesa ispitanika ili druge osobe,
  - obrada je potrebna za obavljanje zadataka od javnog interesa,
  - razlog za obradu su legitimni interesi rukovaoca podacima ili trećih lica, ali samo ako ih ne nadjačavaju interesi ili osnovna prava ispitanika.
- Zakonita obrada osetljivih ličnih podataka podleže posebnom, strožem režimu.

4.1.1. Zakonska osnova obrade podataka

U poglavlju II Opšte uredbe o zaštiti podataka, pod naslovom „Načela", utvrđuje se da svaka obrada ličnih podataka prvenstveno mora da bude u skladu sa načelima kvaliteta podataka iz člana 5. Uredbe. Prema jednom od načela, lični podaci treba da budu „zakonito, pravično i transparentno obrađivani". Zatim, da bi se podaci obradili na zakonit način, obrada mora da bude u skladu sa jednom od zakonskih osnova na osnovu kojih obrada podataka postaje legitimna, a koje su navedene u članu 6.[341] za neosetljive lične podatke odnosno u članu 9. za posebne kategorije podataka (ili osetljive podatke). Slično tome, u poglavlju II modernizovane Konvencije br. 108, u kojem se utvrđuju „osnovna načela zaštite ličnih podataka", propisuje se da obrada podataka mora biti „srazmerna s obzirom na legitimnu svrhu koja treba da se ostvari" da bi bila zakonita.

Nezavisno od zakonske osnove obrade na koju se rukovalac podacima oslanja pri pokretanju postupka obrade ličnih podataka, rukovalac podacima takođe treba da primeni zaštitne mere utvrđene u opštem sistemu zakonodavstva o zaštiti podataka.

Pristanak/Saglasnost

U okviru prava Saveta Evrope, pristanak/saglasnost se spominje u članu 5. stavu 2. modernizovane Konvencije br. 108. Takođe se navodi u sudskoj praksi ESLJP-a i u

341 SPEU, spojeni predmeti C-465/00, C-138/01 i C-139/01, *Rechnungshof protiv Österreichischer Rundfunk i dr. i Christa Neukomm i Joseph Lauermann protiv Österreichischer Rundfunk*, 20. maja 2003, stav 65.; SPEU, C-524/06, *Heinz Huber protiv Bundesrepublik Deutschland* [VV], 16. decembra 2008, stav 48.; SPEU, spojeni predmeti C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) protiv Administración del Estado*, 24. novembra 2011, stav 26.

nekoliko preporuka Saveta Evrope[342]. **U okviru prava EU**, pristanak kao osnova za zakonitu obradu podataka jasno je utvrđena članom 6. OUZP-a i takođe se izričito spominje u članu 8. Povelje. Svojstva valjanog pristanka objašnjena su u definiciji pristanka iz člana 4., uslovi za dobijanje valjanog pristanka detaljno su opisani u članu 7., a posebna pravila o pristanku deteta u vezi s uslugama informatičke kompanije utvrđena su članom 8. OUZP-a.

Kao što je objašnjeno u delu 2.4, pristanak mora biti dat dobrovoljno, utemeljen na informacijama, poseban i nedvosmislen. Pristanak mora biti izjava ili jasan potvrdni čin kojim se pristaje na obradu podataka, a pojedinac ima pravo da ga povuče u bilo kom trenutku. Rukovaoci podacima imaju dužnost vođenja evidencije o pristanku koji se može proveriti.

Dobrovoljni pristanak

U pravnom okviru **Saveta Evrope**, tj. modernizovane Konvencije br. 108, pristanak ispitanika mora „predstavljati slobodan izraz svesne odluke"[343]. Postojanje dobrovoljnog pristanka valjano je samo „ako ispitanik može zaista da bira bez opasnosti od obmane, zastrašivanja, prisile ili ozbiljnih negativnih posledica ako uskrati pristanak"[344]. U tom pogledu, **pravom EU** utvrđeno je da se pristanak ne smatra dobrovoljno datim „ako ispitanik nema istinski ili slobodan izbor ili ako nije u mogućnosti da odbije ili povuče pristanak bez posledica"[345]. U OUZP-u se naglašava da „[k]ada se procenjuje da li je pristanak bio dobrovoljan, u najvećoj mogućoj meri uzima se u obzir da li je, između ostalog, izvršenje ugovora, uključujući pružanje usluge, uslovljeno pristankom za obradu ličnih podataka koji nije nužan za izvršenje tog ugovora"[346]. U Izveštaju s objašnjenjima o modernizovanoj Konvenciji br. 108 navodi se da se „[n]ikakav nedopušteni uticaj ili pritisak (koji može biti ekonomske ili druge prirode), bilo neposredan ili posredan, ne sme izvršiti na ispitanika, a pristanak se ne može smatrati dobrovoljno datim ako ispitanik nema istinski izbor ili nije u mogućnosti da uskrati ili povuče pristanak bez štetnih posledica"[347].

342 Vidi, na primer, Savet Evrope, Komitet ministara (2010), Preporuka CM/Rec(2010)13 Odbora ministara državama članicama o zaštiti pojedinaca u vezi s automatskom obradom ličnih podataka u kontekstu izrade profila, 23. novembra 2010, član 3.4. tačka (b).

343 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 42.

344 Videti i *Mišljenje 15/2011 o pojmu pristanka* Radne grupe iz člana 29. (2011), WP 187, Bruxelles, 13. jula 2011, str. 12.

345 Opšta uredba o zaštiti podataka, uvodna izjava 42.

346 *Ibid*., član 7. stav 4.

347 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 42.

Primer: Određene opštine u državi A odlučile su da uvezu boravišne legitimacije s ugrađenim čipom. Stanovnici opštine nisu obavezni da imaju te elektronske legitimacije. Međutim, stanovnicima koji nemaju legitimaciju uskraćen je pristup nizu važnih administrativnih usluga, poput mogućnosti plaćanja lokalnih poreza putem interneta, podnošenja tužbi elektronskim putem, čime se ostvaruje prednost trodnevnog roka u kojem nadležni organ mora da odgovori, kao i zaobilaženje čekanja u redovima, kupovine ulaznica za gradsku koncertnu dvoranu po nižim cenama i upotrebe uređaja za skeniranje na ulazu.

Obrada ličnih podataka za potrebe opštine u ovom primeru ne može biti zasnovana na pristanku. Budući da se na stanovnike vrši barem posredan pritisak da nabave elektronsku legitimaciju i pristanu na obradu podataka, njihov pristanak nije dobrovoljan. Razvoj sistema elektronskih legitimacija unutar opštine zato treba da se zasniva na drugoj zakonskoj osnovi kojom se opravdava obrada. Na primer, opština se može pozvati na činjenicu da je obrada podataka nužna za izvršavanje zadatka od javnog interesa, što je zakonita osnova za obradu u skladu sa članom 6. stav 1. tačka (e) OUZP-a[348].

Dobrovoljni pristanak takođe može biti doveden u pitanje u situacijama podređenosti, tj. kada postoji značajna ekonomska ili druga neravnoteža između rukovaoca podacima, koji obezbeđuje pristanak, i ispitanika, koji daje pristanak[349]. Tipičan primer takve neravnoteže i podređenosti jeste poslodavčeva obrada ličnih podataka u kontekstu radnog odnosa. Prema mišljenju Radne grupe iz člana 29. „[z]aposleni gotovo nikada nisu u poziciji da dobrovoljno daju, uskrate ili opozovu pristanak s obzirom na zavisnost koja proizlazi iz odnosa poslodavca i zaposlenih. S obzirom na neravnotežu moći, zaposleni mogu da daju dobrovoljni pristanak samo u izuzetnim okolnostima, kada nema nikakvih posledica usled prihvatanja ili odbijanja neke ponude"[350].

348 Radna grupa iz člana 29. (2011), *Mišljenje 15/2011 o pojmu pristanka*, WP 187, Bruxelles, 13. jula 2011., str. 16. Dodatni primeri slučajeva u kojima se obrada podataka ne može temeljiti na pristanku, nego zahteva drugu zakonsku osnovu kojom se opravdava obrada, dostupni su na 14. i 17. str. Mišljenja.

349 Vidi i *Mišljenje 8/2001 o obradi ličnih podataka u kontekstu zaposlenja* Radne grupe iz člana 29. (2001), WP 48, Bruxelles, 13. septembra 2001.; Radna grupa iz člana 29. (2005.), Radni dokument o zajedničkom tumačenju člana 26 stava 1. Direktive 95/46/EZ od 24. oktobra 1995., WP 114, Bruxelles, 25. novembra 2005.; Radna grupa iz člana 29. (2017), *Mišljenje 2/2017 o obradi podataka na radnom mestu*, WP 249, Bruxelles, 8. juna 2017.

350 Radna grupa iz člana 29., Opinion 2/2017 on data processing at work (Mišljenje 2/2017 o obradi podataka na radnom mestu), WP 249, Bruxelles, 8. juna 2017.

Primer: Velika kompanija planira da napravi imenik sa imenima svih zaposlenih, njihovim funkcijama u kompaniji i poslovnim adresama, i to isključivo u svrhe unapređenja unutarnje komunikacije kompanije. Rukovodilac kadrovskom službom predlaže da se u imenik uz svako ime zaposlenog doda i fotografija kako bi se saradnici lakše međusobno prepoznali na sastancima. Predstavnici zaposlenih traže da se to učini isključivo ako na to pristane svaki zaposleni posebno.

U takvoj situaciji pristanak zaposlenih treba priznati kao pravnu osnovu za obradu fotografija u imeniku, jer objava fotografije u imeniku sama po sebi verovatno ne nosi nikakve posledice po zaposlenog, nezavisno od toga da li pristane li na objavu fotografije u imeniku ili ne.

Primer: Kompanija A planira sastanak troje svojih zaposlenih i direktora kompanije B radi razgovora o mogućoj budućoj saradnji na projektu. Sastanak će se održati u poslovnim prostorijama kompanije B, koje od kompanije A traži da mu putem e-pošte dostavi imena, biografije i fotografije učesnika sastanka. Kompanija B tvrdi da su mu imena i fotografije učesnika potrebni kako bi osoblje zaduženo za bezbednost na ulazu u zgradu moglo da proveri da li se radi o pravim osobama, a biografije će direktorima omogućiti da se bolje pripreme za sastanak. U ovom slučaju prenos ličnih podataka zaposlenih kompanije A ne može se zasnivati na pristanku. Pristanak se ne može smatrati dobrovoljnim, jer je moguće da se zaposleni suoče s negativnim posledicama ako odbiju tu ponudu (na primer, mogu da se zamene drugim zaposlenima ne samo na sastanku, nego i u toku dalje saradnje sa kompanijom B i generalno u sklopu projekta). Stoga se obrada mora zasnivati na drugoj zakonitoj osnovi.

Ali to ne znači da pristanak nikada ne može da bude vežeći u okolnostima u kojima bi uskraćivanje pristanka imalo određene negativne posledice. Na primer, ako uskraćivanje pristanka za preuzimanje kartice nekog supermarketa za posledicu ima samo neostvarivanje malog popusta na cene određenih artikala, pristanak ipak može biti važeća pravna osnova za obradu ličnih podataka onih kupaca koji su pristali na preuzimanje kartice. Između kompanije i kupca nema podređenosti, a posledice uskraćivanja pristanka nisu dovoljno ozbiljne da bi sprečile slobodan izbor ispitanika (pod uslovom da je popust na cene dovoljno nizak da ne utiče na njegov slobodan izbor).

Međutim, kada se proizvodi ili usluge mogu dobiti isključivo ako se određeni lični podaci otkriju rukovaocu podacima ili dalje trećim osobama, pristanak ispitanika na otkrivanje sopstvenih podataka koji nisu nužni za taj ugovor ne može se smatrati slobodnom odlukom i zato nije važeća u skladu sa zakonodavstvom o zaštiti podataka[351]. OUZP-om se strogo zabranjuje uslovljavanje davanja proizvoda i usluga davanjem pristanka[352].

Primer: Ako putnici avio-kompanije pristanu da ona prenese takozvane evidencije imena putnika (odnosno podatke o njihovom identitetu, prehrambenim navikama ili zdravstvenim problemima) nadležnim organima za imigraciju određene strane zemlje, to se ne može smatrati valjanim pristankom u skladu sa pravom zaštite podataka, jer putnici nemaju izbora ako žele da posete tu zemlju. Da bi se takvi podaci zakonito preneli, potrebna je druga pravna osnova osim pristanka, a to je najverovatnije poseban zakon.

Pristanak utemeljen na informacijama

Ispitanik mora imati dovoljno informacija pre nego što iskoristi mogućnost izbora. Obično će pristanak utemeljen na informacijama uključivati precizan i vrlo razumljiv opis pitanja za koje se traži pristanak. Kako objašnjava Radna grupa iz člana 29., pristanak se mora zasnivati na uvažavanju i razumevanju činjenica i implikacija radnje ispitanika kojom on pristaje na obradu. Stoga, „[d]otični pojedinac mora na jasan i razumljiv način dobiti tačne i potpune informacije o svim relevantnim pitanjima [...] kao što su priroda podataka koji se obrađuju, svrhe obrade, primaoci podataka i prava ispitanika"[353]. Da bi pristanak bio utemeljen na informacijama, pojedinci takođe moraju biti svesni posledica uskraćivanja pristanka za obradu.

S obzirom na važnost pristanka utemeljenog na informacijama, OUZP-om i Izveštajem s objašnjenjima o modernizovanoj Konvenciji br. 108 nastojalo se da se objasni taj pojam. U uvodnim izjavama OUZP-a utvrđuje se da pristanak utemeljen na infor-

351 Opšta uredba o zaštiti podataka, član 7. stav 4.

352 *Ibid*.

353 Radna grupa iz člana 29. (2007), *Working Document on the processing of personal data relating to health in electronic health records (EHR)* (Radni dokument o obradi ličnih podataka koji se odnose na zdravlje u elektronskim zdravstvenim kartonima), WP 131, Bruxelles, 15. februara 2007.

macijama podrazumeva da bi ispitanik „trebalo [...] barem da zna identitet rukovaoca podacima i svrhe obrade za koju se upotrebljavaju lični podaci"[354].

U izuzetnom slučaju u kojem se pristanak upotrebljava kao odstupanje kako bi se obezbedila zakonita osnova za međunarodni prenos podataka, da bi pristanak bio važeći, rukovalac podacima mora da obavesti ispitanika o mogućim rizicima takvog prenosa zbog nepostojanja odluke o primerenosti i odgovarajućih zaštitnih mera[355].

U Izveštaju s objašnjenjima o modernizovanoj Konvenciji br. 108 utvrđuje se da se moraju dati informacije o implikacijama odluke ispitanika, prvenstveno „šta činjenica davanja saglasnosti podrazumeva i meru u kojoj se saglasnost daje"[356].

Važan je i kvalitet informacija. Kvalitet informacija znači da jezik informacija treba da se prilagodi predviđenim primaocima. Informacije se moraju dati bez žargona, na jasnom i jednostavnom jeziku koji prosečni korisnik može razumeti[357]. Informacije takođe moraju da budu lako dostupne ispitaniku, a mogu se dati usmenim ili pisanim putem. Dostupnost i vidljivost informacija važni su elementi: informacije moraju biti jasno vidljive i istaknute. U elektronskom okruženju dobro rešenje mogu da budu slojevita informativna obaveštenja, jer ona ispitanicima omogućavaju odabir pristupa sažetoj ili proširenoj verziji informacija.

Poseban pristanak

Da bi bio važeći, pristanak takođe mora biti posebno namenjen svrsi obrade, koja mora biti jasno i nedvosmisleno opisana. To ide ruku podruku s kvalitetom informacija pruženih o svrsi pristanka. U tom kontekstu su relevantna razumna očekivanja prosečnog ispitanika. Ako treba dodavati ili menjati postupke obrade na način koji se nije mogao opravdano predvideti u trenutku davanja prvog pristanka, pa je time došlo do promene svrhe, od ispitanika se ponovo mora tražiti pristanak. Kada obrada ima višestruke svrhe, pristanak bi trebalo dati za sve njih[358].

354 Opšta uredba o zaštiti podataka, uvodna izjava 42.

355 *Ibid*., član 49. stav 1. tačka (a).

356 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 42.

357 Radna grupa iz člana 29. (2011), *Opinion 15/2011 on the definition of consent* (Mišljenje 15/2011 o pojmu pristanka), WP 187, Bruxelles, 13. jula 2011, str. 19.

358 Opšta uredba o zaštiti podataka, uvodna izjava 32.

Primeri: U predmetu *Deutsche Telekom AG*[359] SPEU je razmatrao da li je pružalac telekomunikacionih usluga, koji je morao da prosledi lične podatke pretplatnika radi objave u registrima, trebalo da zatraži novi pristanak ispitanika[360] s obzirom na to da primaoci podataka u trenutku davanja pristanka nisu bili navedeni.

SPEU je smatrao da u skladu sa članom 12. Direktive o privatnosti i elektronskim komunikacijama novi pristanak nije potreban pre prosleđivanja podataka. Budući da su ispitanici imali samo mogućnost da daju pristanak za svrhu obrade, odnosno objavu njihovih podataka, nisu mogli da odaberu registar u kojem bi se ti podaci mogli objaviti.

SPEU je istakao kako „iz kontekstualnog i sistemskog tumačenja člana 12. Direktive o privatnosti i elektronskim komunikacijama proizlazi da se saglasnost iz člana 12. stav 2. odnosi na svrhu objave ličnih podataka u javnom imeniku, a ne na identitet konkretnog pružaoca usluge imenika"[361]. Zatim, „sama objava ličnih podataka u javnom imeniku u posebne svrhe se može pokazati štetnom za pretplatnika"[362], a ne identitet autora objave.

Predmet *Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV protiv Autoriteit Consument en Markt (ACM)*[363] odnosio se na zahtev belgijske kompanije za pristup podacima u vezi sa pretplatnicima usluge davanja obaveštenja o brojevima pretplatnika i telefonskih imenika putem kojih se dodeljuju telefonski brojevi u Holandiji. Belgijska kompanija se oslonila na obavezu utvrđenu Direktivom o univerzalnoj usluzi[364]. Prema njoj, kompanije koje dodeljuju telefonske brojeve obavezne su da učine brojeve dostupnima telefonskim imenicima koji ih zatraže ako pretplatnici daju pristanak za objavu svojih brojeva. Holandske kompanije su to odbile, tvrdeći da ne moraju da daju

359 SPEU, C-543/09, *Deutsche Telekom AG protiv Bundesrepublik Deutschland*, 5. maja 2011. Videti posebno st. 53 i 54.

360 Direktiva 2002/58/EZ Evropskog parlamenta i Saveta od 12. jula 2002. o obradi ličnih podataka i zaštiti privatnosti u oblasti elektronskih komunikacija, SL 2002 L 201 (Direktiva o privatnosti i elektronskim komunikacijama).

361 SPEU, C-543/09, *Deutsche Telekom AG protiv Bundesrepublik Deutschland*, 5. maja 2011, stav 61.

362 *Ibid*., stav 62.

363 SPEU, C-536/15, *Tele2 (Netherlands) BV i dr. protiv Autoriteit Consument en Markt (ACM)*, 15. marta 2017.

364 Direktiva 2002/22/EZ Evropskog parlamenta i Saveta od 7. marta 2002. o univerzalnoj usluzi i pravima korisnika u vezi s elektronskim komunikacionim mrežama i uslugama (Direktiva o univerzalnoj usluzi), SL 2002 L 108, str. 51, kako je izmenjena Direktivom 2009/136/EZ Evropskog parlamenta i Saveta od 25. novembra 2009. (Direktiva o univerzalnim uslugama), SL 2009 L 337, str. 11.

predmetne podatke preduzeću koje ima sedište u drugoj državi članici. Tvrdile su da su korisnici dali pristanak za objavu svojih brojeva smatrajući da će se oni objaviti u holandskom telefonskom imeniku. SPEU je zaključio da se Direktivom o univerzalnoj usluzi obuhvataju svi zahtevi preduzeća koja pružaju usluge davanja obaveštenja o brojevima pretplatnika, nezavisno od države članice u kojoj imaju sedište. Takođe je zaključio da se prosleđivanjem tih podataka drugom preduzeću s namerom objave javnog telefonskog imenika bez dobijanja novih pristanka pretplatnika ne može značajno narušiti pravo na zaštitu ličnih podataka[365]. Stoga, nije nužno da preduzeće koje dodeljuje telefonske brojeve pretplatnicima u svom zahtevu za pristanak pretplatnika posebno navodi državu članicu u koju se podaci o njemu mogu poslati[366].

Nedvosmisleni pristanak

Svaki pristanak se mora dati nedvosmisleno[367]. To znači da ne sme izazivati opravdanu sumnju da je ispitanik želeo da izrazi svoje slaganje s obradom svojih podataka. Na primer, neaktivnost ispitanika ne podrazumeva nedvosmisleni pristanak.

To bi bio slučaj kada rukovalac podacima izdejstvuje pristanak izjavama u svojim pravilima zaštite privatnosti poput „upotrebom naše usluge pristajete na obradu svojih ličnih podataka". U takvom slučaju će rukovaoci podacima možda morati da osiguraju da korisnici ručno i pojedinačno pristanu na takva pravila.

Ako se pristanak daje u okviru obrasca koji je deo ugovora, pristanak za obradu ličnih podataka mora biti individualizovan, a u svakom slučaju, „zaštitnim merama [...] trebalo bi obezbediti da je ispitanik svestan činjenice da daje pristanak i do koje mere se on daje"[368].

Zahtevi pristanka za decu

OUZP-om se propisuje posebna zaštita dece u kontekstu pružanja usluga informatičke kompanije, budući da ona „mogu biti manje svesna rizika, posledica i predmet-

365 SPEU, C-536/15, *Tele2 (Netherlands) BV i dr. protiv Autoriteit Consument en Markt (ACM)*, 15. marta 2017, stav 36.

366 *Ibid*., st. 40 i 41.

367 Opšta uredba o zaštiti podataka, član 4. stav 11.

368 *Ibid*., uvodna izjava 42.

nih zaštitnih mera te svojih prava u vezi s obradom ličnih podataka"[369]. U skladu sa **pravom EU**, kada pružaoci usluga informatičke kompanije obrađuju lične podatke dece mlađe od 16 godina na osnovu pristanka, takva je obrada zakonita „samo ako i u meri u kojoj je pristanak dao ili odobrio nosilac starateljstva nad detetom"[370]. Države članice mogu propisati niži uzrast u domaćem zakonodavstvu, ali ne niži od 13 godina[371]. Pristanak nosioca starateljstva nije nužan „u kontekstu preventivnih usluga ili usluga savetovanja koje su ponuđene neposredno detetu"[372]. Informacije i komunikacija, u slučaju da je obrada usmerena prema detetu, trebalo bi da budu na jasnom i jednostavnom jeziku koji dete lako može razumeti[373].

Pravo na povlačenje pristanka u svakom trenutku

OUZP sadrži opšte pravo na povlačenje pristanka u svakom trenutku[374]. Ispitanik mora biti obavešten o takvom pravu pre davanja pristanka i on može iskoristiti to pravo prema sopstvenom nahođenju. Ne bi trebalo da se postavljaju zahtevi za obrazloženje povlačenja niti bi smelo da bude rizika od negativnih posledica, osim ukidanja svih povlastica koje su proizlazile iz prethodno dogovorene upotrebe podataka. Povlačenje pristanka treba da bude podjednako jednostavno kao njegovo davanje[375]. Dobrovoljni pristanak nije moguć ako ispitanik ne može da povuče svoj pristanak bez štetnih posledica ili ako povlačenje nije podjednako jednostavno kao davanje pristanka[376].

Primer: Kupac pristane na primanje reklamnih poruka na adresu koju je dostavio rukovaocu podacima. Ako kupac povuče pristanak, rukovalac podacima mora odmah da prestane sa slanjem takvih reklamnih poruka. Ne smeju da se nameću nikakve kaznene mere kao što su naknade. Povlačenje se odnosi na budućnost i nema retroaktivan efekat. Period u kojem su se lični podaci kupca

369 *Ibid*., uvodna izjava 38.

370 *Ibid*. Član 8. stav 1. prva alineja. Pojam usluga informatičke kompanije definisan je u članu 4. stav 25. Opšte uredbe o zaštiti podataka.

371 Opšta uredba o zaštiti podataka, član 8. stav 1. druga alineja.

372 *Ibid*., uvodna izjava 38.

373 *Ibid*., uvodna izjava 58. Vidi i modernizovanu Konvenciju br. 108, član 15. stav 2. tačka (e). Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, st. 68 i 125.

374 Opšta uredba o zaštiti podataka, član 7. stav 3. Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 45.

375 Opšta uredba o zaštiti podataka, član 7. stav 3.

376 Opšta uredba o zaštiti podataka, uvodna izjava 42; Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 42.

zakonito obrađivali bio je legitiman zahvaljujući pristanku kupca. Povlačenjem se sprečava svaka dalja obrada tih podataka, osim ako je ona u skladu sa pravom na brisanje[377].

Nužnost za izvršavanje ugovora

Prema pravu EU, članom 6. stav 1. tačka (b) OUZP-a utvrđuje se dodatna osnova za zakonitu obradu, a to je da je obrada „nužna za izvršavanje ugovora u kojem je ispitanik stranka". Ta odredba obuhvata i predugovorne odnose. Na primer, u slučajevima u kojima stranka namerava da sklopi ugovor, ali to još nije učinila, možda jer je potrebno obaviti još neke provere. Ako jedna stranka treba da obradi podatke u tu svrhu, takva obrada je zakonita sve dok je nužna „kako bi se preduzele radnje na zahtev ispitanika pre sklapanja ugovora"[378].

Ideja obrade podataka kao „legitimne osnove propisane zakonom" iz člana 5. stav 2. modernizovane Konvencije br. 108 takođe obuhvata „obradu podataka u svrhu izvršavanja ugovora (ili predugovornih mera na zahtev lica čiji se podaci obrađuju) u kojima je ispitanik stranka"[379].

Pravne dužnosti rukovaoca podacima

U pravu EU utvrđuje se još jedna osnova za postizanje legitimnosti obrade podataka, i to ako je obrada „nužna radi poštovanja pravnih obaveza rukovaoca podacima" (član 6. stav 1. tačka (c) OUZP-a). Ova odredba se odnosi na rukovaoce podacima koji deluju i u privatnom i u javnom sektoru. Pravne obaveze rukovaoca podacima iz javnog sektora takođe mogu potpadati pod član 6. stav 1. tačka (e) OUZP-a. Mnogo je slučajeva u kojima su rukovaoci podacima iz privatnog sektora zakonom obavezani da obrađuju podatke o pojedinim ispitanicima. Na primer, poslodavci moraju da obrađuju podatke o svojim zaposlenima za potrebe socijalnog osiguranja i oporezivanja, a preduzeća moraju da obrađuju podatke o svojim klijentima radi oporezivanja.

377 Opšta uredba o zaštiti podataka, član 17. stav 1. tačka (b).

378 *Ibid*., član 6. stav 1. tačka (b).

379 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 46, Savet Evrope, Savet ministara (2010), Preporuka CM/Rec(2010)13 Odbora ministara državama članicama o zaštiti pojedinaca u vezi s automatskom obradom ličnih podataka u kontekstu izrade profila, 23. novembra 2010, član 3.4. tačka (b).

Pravna obaveza može proizlaziti iz prava Unije ili države članice, koje može biti osnova za jedan ili više postupaka obrade. Zakonom treba da se utvrde svrha obrade, specifikacije za utvrđivanje rukovaoca podacima, vrste ličnih podataka koji podležu obradi, dotičnih ispitanika, subjekata kojima se lični podaci mogu otkriti, ograničenja svrhe, perioda čuvanja i drugih mera za obezbeđivanje zakonite i pravične obrade[380]. Svaki takav zakon, koji predstavlja osnovu za obradu podataka, mora biti u skladu sa članovima 7. i 8. Povelje i članom 8. EKLJP-a.

Pravne obaveze rukovaoca podacima predstavljaju osnovu za zakonitu obradu podataka i unutar **prava Saveta Evrope**[381]. Kao što je prethodno navedeno, pravne obaveze rukovaoca podacima iz privatnog sektora samo su jedan poseban slučaj legitimnih interesa drugih, kao što je navedeno u članu 8. stavu 2. EKLJP-a. Stoga je primer u kojem poslodavci obrađuju lične podatke zaposlenih relevantan i za pravo Saveta Evrope.

Vitalni interesi ispitanika ili drugog fizičkog lica

Prema pravu EU, članom 6 stav 1. tačka (d) OUZP-a propisuje se da je obrada ličnih podataka zakonita ako je „nužna kako bi se zaštitili ključni interesi ispitanika ili drugog fizičkog lica". Ta legitimna osnova se može primeniti samo na obradu ličnih podataka na osnovu životno važnih interesa drugog fizičkog lica ako takva obrada „očigledno ne može da se temelji na drugoj pravnoj osnovi"[382]. Ponekad se vrsta obrade može temeljiti na osnovi javnog interesa i vitalnih interesa ispitanika ili drugog lica. Na primer, to je slučaj pri praćenju epidemija i njihovg razvoja ili pojave humanitarne krize.

Unutar prava Saveta Evrope vitalni interesi ispitanika ne spominju se u članu 8. EKLJP-a. Međutim, smatra se da se vitalni interesi ispitanika podrazumevaju u sklopu pojma „legitimne osnove" iz člana 5. stav 2. modernizovane Konvencije br. 108, koji se odnosi na legitimnost obrade ličnih podataka[383].

380 Opšta uredba o zaštiti podataka, uvodna izjava 45.

381 Savet Evrope, Komitet ministara (2010), Preporuka CM/Rec(2010)13 Savetaministara državama članicama o zaštiti pojedinaca u vezi s automatskom obradom ličnih podataka u kontekstu izrade profila, 23. novembra 2010, član 3.4. tačka (a).

382 Opšta uredba o zaštiti podataka, uvodna izjava 46.

383 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 46.

Javni interes i izvršavanje javnog ovlašćenja

S obzirom na to da se javni poslovi mogu organizovati na mnoge načine, članom 6. stav 1. tačka (e) OUZP-a propisano je da se lični podaci mogu zakonito obraditi ako je obrada „nužna za izvršavanje zadatka od javnog interesa ili pri izvršavanju službenog ovlašćenja rukovaoca podacima [...]"[384].

Primer: U predmetu *Huber protiv Bundesrepublik Deutschland*[385] g. Huber, austrijski državljanin s prebivalištem u Nemačkoj, zatražio je od Savezne kancelarije za migracije i izbeglice da izbriše podatke o njemu iz Centralnog registra stranih državljana („AZR"). Taj registar, u kojem su sadržani lični podaci o stanovnicima Evropske unije koji nisu nemački državljani, ali borave u Nemačkoj duže od tri meseca, koristi se u statističke svrhe i upotrebljavaju ga policijska i pravosudna tela u istrazi i gonjenju krivičnih dela ili onih koje ugrožavaju javnu bezbednost. Sud koji se obratio SPEU postavio je pitanje da li je obrada ličnih podataka koju obavlja registar poput Centralnog registra stranih državljana, kojem mogu da pristupe i druga javna tela, u skladu s pravom Unije s obzirom na to da takav registar ne postoji za nemačke državljane.

SPEU je smatrao da se prema članu 7. tačka (e) Direktive 95/46/EZ[386] lični podaci mogu zakonito obrađivati ako je to nužno za izvršavanje zadatka koji se sprovodi zbog javnog interesa ili pri izvršavanju javnog ovlašćenja.

Prema mišljenju SPEU, „u pogledu cilja obezbeđenja jednakog nivoa zaštite u svim državama članicama, [...] pojam potrebe, onako kako proizlazi iz člana 7. tačka (e) Direktive 95/46[387], ne može imati različit sadržaj u zavisnosti od država članica. Iz toga proizlazi da se radi o pojmu koji ima sopstveno nezavisno značenje u pravu Zajednice i koji treba tumačiti na način kojim se u potpunosti održava cilj te direktive, kako je naveden u njenom članu 1. stav 1."[388].

SPEU je napomenuo da pravo na slobodu kretanja građana Unije na području države članice čiji nisu državljani nije bezuslovno, već može da podleže

384 Videti Opštu uredbu o zaštiti podataka, uvodna izjava 45.

385 SPEU, C-524/06, *Heinz Huber protiv Bundesrepublik Deutschland* [VV], 16. decembra 2008.

386 Nekadašnja Direktiva o zaštiti podataka, član 7. tačka (e), sada Opšta uredba o zaštiti podataka, član 6. stav 1. tačka (e).

387 *Ibid*.

388 SPEU, C-524/06, *Heinz Huber protiv Bundesrepublik Deutschland* [VV], 16. decembra 2008, stav 52.

ograničenjima i uslovima utvrđenim u Ugovoru o osnivanju Evropske zajednice i merama donesenim radi njegovog sprovođenja. Dakle, ako je, u načelu, zakonito da država članica upotrebljava registar poput AZR-a radi podrške telima odgovornim za primenu zakonodavstva povezanog s pravom boravka, takav registar ne sme da sadrži informacije koje nisu nužne za tu određenu svrhu. SPEU je zaključio da je takav sistem obrade ličnih podataka u skladu s pravom EU ako sadrži samo one podatke koji su potrebni za primenu tog zakonodavstva i ako je zbog njegove centralizovane prirode primena tog zakonodavstva efikasnija. Domaći sud mora utvrditi da li su ti uslovi ispunjeni u ovom konkretnom slučaju. Ako nisu, čuvanje i obrada ličnih podataka u registru poput AZR-a u statističke svrhe ne mogu se ni po kojoj osnovi smatrati nužnim u smislu člana 7. tačka (e)[389] Direktive 95/46/EZ[390].

Na kraju, što se tiče pitanja upotrebe podataka sadržanih u registru u svrhu suzbijanja kriminala, SPEU je smatrao da taj cilj „nužno uključuje gonjenje učinjenih zločina ili krivičnih dela, nezavisno od državljanstva učinioca". Predmetni registar ne sadrži lične podatke povezane s državljanima predmetne države članice i ta razlika u postupanju predstavlja diskriminaciju koja je zabranjena članom 18. UFEU. Stoga je SPEU zaključio da se tom odredbom, „isključuje mogućnost da država članica, u svrhu suzbijanja kriminala, uspostavi sistem za obradu ličnih podataka posebno za stanovnike Unije koji nisu državljani te države članice"[391].

Upotreba ličnih podataka onih tela koja deluju u javnoj sferi, takođe, podleže članu 8. **EKLJP-a**, te je predviđeno da bude obuhvaćena članom 5. stav 2. modernizovane Konvencije br. 108 kada je to primenjivo[392].

Legitimni interesi rukovaoca podacima ili treće strane

Prema **pravu EU**, ispitanik nije jedini koji ima legitimne interese. Članom 6. stav 1. tačka (f) OUZP-a propisano je da se podaci mogu zakonito obraditi ako je obrada „nužna za potrebe legitimnih interesa rukovaoca podacima ili treće strane [osim tela

389 Nekadašnja Direktiva o zaštiti podataka, član 7. tačka (e), sada Opšta uredba o zaštiti podataka, član 6. stav 1. tačka (e).

390 SPEU, C-524/06, *Heinz Huber protiv Bundesrepublik Deutschland* [VV], 16. decembra 2008, st. 54, 58, 59 i od 66 do 68.

391 *Ibid*., st. 78 i 81.

392 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, st. 46 i 47.

javne vlasti pri izvršavanju njihovih zadataka], kojima se podaci otkrivaju, osim kada su od tih interesa jači interesi ili osnovna prava i slobode ispitanika koji zahtevaju zaštitu [...]"[393].

Postojanje legitimnog interesa mora se pažljivo proceniti u svakom pojedinačnom slučaju[394]. Ako se utvrde legitimni interesi rukovalaca podacima, mora se sprovesti postupak procene tih interesa i interesa ili osnovnih prava i sloboda ispitanika[395]. Tokom takve procene moraju se uzeti u obzir razumna očekivanja ispitanika kako bi se utvrdilo da li interesi nadvladavaju interese rukovaoca podacima ili osnovna prava ispitanika[396]. Ako prava ispitanika nadvladavaju legitimne interese rukovaoca podacima, rukovalac podacima može preduzeti određene mere i primeniti zaštitne mere kako bi obezbedio što manji efekat na prava ispitanika (kao što je pseudonimizacija podataka) i preokrenuti „ravnotežu" pre nego što se bude mogao zakonito osloniti na tu legitimnu osnovu obrade. U Mišljenju o pojmu legitimnih interesa rukovaoca podacima, Radna grupa iz člana 29. istakla je ključnu ulogu odgovornosti i transparentnosti, kao i prava ispitanika na prigovor na obradu svojih podataka, ili na pristup tim podacima, njihovu izmenu, brisanje ili prenos, u proceni legitimnih interesa rukovaoca podacima i interesa osnovnih prava ispitanika[397].

U uvodnim izjavama OUZP-a daju se primeri onoga što čini legitimni interes dotičnog rukovaoca podacima. Na primer, obrada ličnih podataka dopuštena je bez pristanka ispitanika kada se vrši u svrhe neposrednog marketinga ili kada je takva obrada „nužna u svrhe sprečavanja prevara"[398].

U svojoj sudskoj praksi SPEU je proširio procenu/test kojom se utvrđuje šta čini legitiman interes.

393 U odnosu na Direktivu 95/46/EZ, u Opštoj uredbi o zaštiti podataka daje se više primera slučajeva za koje se smatra da predstavljaju legitiman interes.

394 Opšta uredba o zaštiti podataka, preambula, uvodna izjava 47.

395 Radna grupa iz člana 29. (2014), *Mišljenje 06/2014 o pojmu legitimnih interesa rukovaoca podacima u skladu s članom 7. Direktive 95/46/EZ*, WP 217, 4. aprila 2014.

396 *Ibid*.

397 *Ibid*.

398 Opšta uredba o zaštiti podataka, preambula, uvodna izjava 47.

Primer: Predmet *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde*[399] odnosio se na štetu koju je putnik naglim otvaranjem vrata taksija naneo trolejbusu prevozničkog preduzeća u gradu Rigi. Kompanija Rīgas satiksme htela je da tuži putnika taksija radi dobijanja odštete. Međutim, policija je dala samo ime putnika i uskratila njegov identifikacioni broj i adresu, tvrdeći da bi takvo otkrivanje podataka bilo nezakonito prema domaćim zakonima o zaštiti podataka.

Letonski sud zatražio je da SPEU donese prethodnu odluku o tome da li se pravom zaštiti podataka EU nameće obaveza saopštavanja svih ličnih podataka potrebnih za pokretanje građanske parnice protiv osobe koja je navodno odgovorna za počinjenje zakonskog prekršaja[400].

SPEU je obrazložio da se pravom zaštite podataka EU propisuje mogućnost – a ne obaveza – saopštavanja podataka trećim stranama radi ostvarenja njihovih zakonitih interesa[401]. SPEU je utvrdio tri kumulativna uslova koji se moraju ispuniti kako bi obrada ličnih podataka bila zakonita na osnovi „zakonitih interesa"[402]. Prvo, treća strana kojoj se podaci otkrivaju mora imati zakonit interes. U ovom konkretnom slučaju, to znači da traženje ličnih podataka radi utuživanja osobe zbog štete na imovini predstavlja zakonit interes treće strane. Drugo, obrada ličnih podataka mora biti nužna za ostvarenje tih zakonitih interesa. U ovom slučaju, dobijanje ličnih podataka kao što su adresa i/ili identifikacioni broj strogo je nužno za identifikaciju dotične osobe. Treće, osnovna prava i slobode ispitanika ne smeju da imaju prednost nad zakonitim interesima rukovaoca podacima ili trećih strana. Balansiranje interesa mora se sprovesti za svaki pojedinačni slučaj, uzimajući u obzir elemente poput težine kršenja prava ispitanika ili čak uzrasta ispitanika u određenim okolnostima. Međutim, u ovom slučaju SPEU nije smatrao da je odbijanje otkrivanja podataka opravdano isključivo zbog činjenice da je ispitanik maloletan.

399 SPEU, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde protiv Rīgas pašvaldības SIA „Rīgas satiksme"*, 4. maja 2017.

400 *Ibid.*, stav 23.

401 *Ibid.*, stav 26.

402 *Ibid.*, st. od 28 do 34.

U predmetu *ASNEF i FECEMD* SPEU je presudu doneo isključivo o obradi podataka na osnovu zakonite osnove „legitimnih interesa", koja je u to vreme bila utvrđena u članu 7. tačka (f) Direktive o zaštiti podataka[403].

Primer: U predmetu *ASNEF i FECEMD*[404] SPEU je objasnio da se u domaćem zakonodavstvu ne smeju dodavati uslovi onima navedenima u članu 7. tačka (f) Direktive za zakonitu obradu podataka[405]. To se odnosilo na situaciju u kojoj je španski zakon o zaštiti podataka sadržao odredbu na osnovu koje bi druge privatne strane mogle da tvrde da imaju legitiman interes u obradi ličnih podataka samo ako su se informacije već pojavile u javnim izvorima.

SPEU je prvo napomenuo da je cilj Direktive 95/46/EZ[406] da obezbedi isti nivo zaštite prava i sloboda pojedinaca u vezi s obradom ličnih podataka u svim državama članicama. Osim toga, usklađivanjem domaćih zakonodavstava primenjivih u toj oblasti ne sme se umanjiti nivo zaštite. Naprotiv, njima se mora nastojati da se obezbedi visok nivo zaštite u EU[407]. Zato je SPEU zaključio da „iz cilja obezbeđivanja jednakog nivoa zaštite u svim državama članicama proizlazi da se članom 7. Direktive 95/46[408] navodi iscrpan i ograničen popis slučajeva u kojima je obradu ličnih podataka moguće smatrati zakonitom". Osim toga, „države članice ne mogu dodavati nova načela koja se odnose na zakonitost obrade ličnih podataka u član 7. Direktive 95/46,[409] niti nametati dodatne zahteve koji deluju tako da izmenjuju opseg primene jednog od šest načela" iz člana 7.[410] SPEU je potvrdio da je u pogledu procene koja je potrebna prema članu 7. tačka (f) Direktive 95/46/EZ moguće uzeti u obzir činjenicu da se ozbiljnost

403 Nekadašnja Direktiva o zaštiti podataka, član 7. tačka (f), sada Opšta uredba o zaštiti podataka, član 6. stav 1. tačka (f).

404 SPEU, spojeni predmeti C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) protiv Administración del Estado*, 24. novembra 2011.

405 Nekadašnja Direktiva o zaštiti podataka, član 7. tačka (f), sada Opšta uredba o zaštiti podataka, član 6. stav 1. tačka (f).

406 Nekadašnja Direktiva o zaštiti podataka, sada Opšta uredba o zaštiti podataka.

407 SPEU, spojeni predmeti C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) protiv Administración del Estado*, 24. novembra 2011, stav 28. Videti Direktivu o zaštiti podataka, uvodne izjave 8 i 10.

408 Nekadašnja Direktiva o zaštiti podataka, član 7., sada Opšta uredba o zaštiti podataka, član 6. stav 1. tačka (f).

409 Nekadašnja Direktiva o zaštiti podataka, član 7., sada Opšta uredba o zaštiti podataka, član 6.

410 *Ibid*.

povrede osnovnih prava ispitanika, koja proizlaze iz obrade, može razlikovati u zavisnosti od toga da li se predmetni podaci već pojavljuju u javnim izvorima.

Međutim, prema članu 7. tačka (f) Direktive „nije moguće da država članica kategorički i generalno isključi mogućnost obrade određenih kategorija ličnih podataka, a da pri tome ne omogući uzajamno uravnoteženje predmetnih suprotnih prava i interesa u konkretnom slučaju".

S obzirom na navedeno, SPEU je zaključio da član 7. tačka (f) Direktive 95/46/EZ[411] treba tumačiti kao da „isključuje domaća pravila koja, u slučaju nepostojanja saglasnosti ispitanika, a radi omogućavanja obrade ličnih podataka ispitanika, koja je nužna da bi se ispunili legitimni interesi rukovaoca podacima ili treće strane ili trećih strana kojima se ti podaci otkrivaju, iziskuju ne samo poštovanje osnovnih prava i sloboda ispitanika, već i pojavljivanje podataka u javnim izvorima. Na taj način se kategorički i generalno isključuje obrada podataka koji se ne pojavljuju u takvim izvorima"[412].

Kad god se lični podaci obrađuju po osnovu „legitimnih interesa", pojedinac ima pravo prigovora na obradu u svakom trenutku na osnovi povezanoj s njegovim konkretnim slučajem, u skladu s članom 21. stav 1. OUZP-a. Rukovalac podacima mora obustaviti obradu, osim ako uverljivo dokaže postojanje legitimne osnove za njen nastavak.

Kad je reč o **pravu Saveta Evrope**, slične formulacije se mogu pronaći u modernizovanoj Konvenciji br. 108[413] i preporukama Saveta. U Preporuci o izradi profila potvrđuje se da je obrada ličnih podataka u svrhe izrade profila zakonita ako je nužna radi legitimnih interesa drugih, „osim kada su ti interesi podređeni temeljnim pravima i slobodama ispitanika"[414]. Usto, „zaštita prava i sloboda drugih" spominje se u članu 8. stav 2. EKLJP-a kao jedna od legitimnih osnova za ograničenje prava na zaštitu podataka.

411 Nekadašnja Direktiva o zaštiti podataka, član 7. tačka (f), sada Opšta uredba o zaštiti podataka, član 6. stav 1. tačka (f).

412 SPEU, spojeni predmeti C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) protiv Administración del Estado*, 24. novembra 2011., st. 40, 44, 48 i 49.

413 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 46.

414 Savet Evrope, Komitet ministara (2010.), *Recommendation CM/Rec(2010)13 and explanatory memorandum on the protection of individuals with regard to automatic processing of personal data in the context of profiling* (Preporuka CM/Rec(2010)13 i Memorandum s objašnjenjima o zaštiti pojedinaca u vezi s automatskom obradom ličnih podataka u kontekstu izrade profila), 23. novembra 2010, član 3.4. tačka (b) (Preporuka o izradi profila).

Primer: U predmetu *Y protiv Turske*[415] podnosilac predstavke je bio HIV pozitivan. Budući da je bio onesvešćen pri dolasku u bolnicu, osoblje hitne pomoći obavestilo je osoblje bolnice da je on HIV pozitivan. Podnosilac predstavke je pred ESLJP-om tvrdio da je otkrivanjem tih informacija prekršeno njegovo pravo na poštovanje privatnog života. Međutim, uzimajući u obzir potrebu za zaštitom bezbednosti bolničkog osoblja, deljenje tih informacija nije se smatralo povredom njegovih prava.

4.1.2. Obrada posebnih kategorija podataka (osetljivih podataka)

Prema pravu Saveta Evrope, domaćim zakonodavstvom se utvrđuje odgovarajuća zaštita za upotrebu osetljivih podataka, pod uslovom da su ispunjeni uslovi iz člana 6. modernizovane Konvencije br. 108, prvenstveno da su odgovarajuće zaštitne mere, koje dopunjuju druge odredbe Konvencije, propisane zakonom. **Pravo Unije,** tj. član 9. OUZP-a, sadrži detaljan režim obrade posebnih kategorija podataka (koji se nazivaju i „osetljivim podacima"). To su podaci kojima se otkriva rasno ili etničko poreklo, politička mišljenja, verska ili filozofska uverenja ili članstvo u sindikatu, a uključuju i genetski podaci, biometrijski podaci za potrebe jedinstvene identifikacije pojedinca, podaci koji se odnose na zdravlje, polni život ili seksualnu orijentaciju pojedinca. Obrada osetljivih podataka u načelu je zabranjena[416].

Međutim, u članu 9 stav 2. Uredbe postoji iscrpan popis izuzetakaod te zabrane, koji čine zakonite osnove za obradu osetljivih podataka. Ta izuzeća uključuju sledeće situacije:

- ispitanik da izričiti pristanak za obradu podataka,
- obradu vrši neprofitna organizacija s političkim, filozofskim, verskim ili sindikalnim ciljem u sklopu svojih legitimnih aktivnosti, tako da se ona odnosi samo na (bivše) članove organizacije ili na osobe koje imaju redovan kontakt s njom u vezi s takvim svrhama,
- obrada se odnosi na lične podatke koje je izričito objavio ispitanik,

415 ESLJP, *Y protiv Turske*, br. 648/10, 17. februara 2015.

416 Nekadašnja Direktiva o zaštiti podataka, član 7. tačka (f), sada Opšta uredba o zaštiti podataka, član 9. stav 1.

- obrada je nužna:
  - za potrebe izvršavanja obaveza i ostvarivanja posebnih prava rukovaoca podacima ili ispitanika u kontekstu zaposlenja, socijalne bezbednosti i socijalne zaštite,
  - za zaštitu životno važnih interesa ispitanika ili drugog fizičkog lica (kada ispitanik nije u mogućnosti da dâ pristanak),
  - za uspostavljanje, ostvarivanje ili odbranu pravnih zahteva ili kad god sudovi deluju u svom pravosudnom svojstvu,
  - u svrhu preventivne medicine ili medicine rada: „radi procene radne sposobnosti zaposlenih, medicinske dijagnoze, pružanja zdravstvene ili socijalne brige ili tretmana ili upravljanja zdravstvenim ili socijalnim sistemima i uslugama na osnovu prava Unije ili prava države članice ili u skladu s ugovorom sa zdravstvenim radnikom",
  - za potrebe arhiviranja u javnom interesu, u svrhe naučnog ili istorijskog istraživanja ili u statističke svrhe,
  - u svrhu javnog interesa u oblasti javnog zdravlja ili
  - za potrebe značajnog javnog interesa.

Zato se za obradu posebnih kategorija podataka ugovorni odnos s ispitanikom ne smatra pravnom osnovom za zakonitu obradu osetljivih podataka, osim ugovora sa zdravstvenim radnikom koji je obavezan da čuva profesionalnu tajnu[417].

Izričit pristanak ispitanika

Prema **pravu Unije**, prvi uslov za zakonitu obradu bilo kojih podataka, neosetljivih ili osetljivih, jeste pristanak ispitanika. U slučaju osetljivih podataka pristanak mora da bude izričit. Međutim, zakonodavstvom Unije ili pojedinih država članica može se propisati da pojedinac ne sme da ukine zabranu obrade posebnih kategorija podataka[418]. Na primer, to može važiti u slučaju kada obrada uključuje neuobičajene rizike za ispitanika.

417 Opšta uredba o zaštiti podataka, član 9. stav 2. tačke (h) i (i).

418 *Ibid.*, član 9. stav 2. tačka (a).

Radno pravo ili pravo o socijalnoj bezbednosti i socijalnoj zaštiti

Prema **pravu Unije**, zabrana iz člana 9. stav 1. može se ukinuti ako je obrada nužna za izvršavanje obaveza ili ostvarivanje prava rukovaoca podacima ili ispitanika u oblasti zaposlenja ili socijalne bezbednosti. Međutim, obrada mora biti odobrena u okviru prava Unije, domaćeg prava ili kolektivnog ugovora u skladu s domaćim pravom, koji pružaju odgovarajuće zaštitne mere za osnovna prava i interese ispitanika[419]. Evidencija o zaposlenju koju vodi neka organizacija može sadržati osetljive lične podatke koji su u određenim uslovima utvrđeni u OUZP-u i relevantnom domaćem pravu. Primeri osetljivih podataka mogu uključivati članstvo u sindikatu ili zdravstvene informacije.

Vitalni interesi ispitanika ili druge osobe

Prema **pravu EU** osetljivi podaci mogu se, kao i neosetljivi podaci, obrađivati zbog vitalnih interesa ispitanika ili drugog fizičkog lica[420]. Kada se obrada zasniva na vitalnim interesima druge osobe, ta zakonita osnova može da se primeni samo ako takva obrada „očigledno ne može da se zasniva na drugoj pravnoj osnovi"[421]. U nekim slučajevima obradom ličnih podataka mogu da se zaštite javni i privatni interesi, na primer kada je obrada potrebna u humanitarne svrhe[422].

Da bi obrada osetljivih podataka bila legitimna na toj osnovi, traženje pristanka od ispitanika mora biti onemogućeno, na primer jer je ispitanik u nesvesti ili odsutan i nedostupan. Drugim rečima, ta osoba mora biti fizički ili pravno nesposobna za davanje pristanka.

419 Opšta uredba o zaštiti podataka, član 9. stav 2. tačka (b).

420 *Ibid*., član 9. stav 2. tačka (c).

421 *Ibid*., uvodna izjava 46.

422 *Ibid.*

Humanitarna udruženja ili neprofitne organizacije

Obrada ličnih podataka dopuštena je i u sklopu legitimnih aktivnosti fondacija, udruženja ili drugih neprofitnih organizacija s političkim, filozofskim, verskim ili sindikalnim ciljem. Međutim, obrada se mora odnositi samo na članove ili bivše članove organizacije ili na osobe koje imaju redovan kontakt s organizacijom[423]. Osetljivi podaci ne smeju da se otkrivaju izvan tih organizacija bez pristanka ispitanika.

Podaci koje očigledno objavljuje ispitanik

U članu 9 stav 2. tačka (e) OUZP-a navodi se da obrada nije zabranjena ako se odnosi na podatke za koje je očigledno da ih je objavio ispitanik. Iako značenje izraza „očigledno da ih je objavio ispitanik" nije definisano u Uredbi, budući da se radi o izuzeću od zabrane obrade osetljivih podataka, mora se strogo tumačiti tako da se od ispitanika zahteva da sa namerom objavi svoje lične podatke. Zato kada se u sklopu televizijskog prenosa prikaže video-zapis snimljen kamerom video-nadzora koji, između ostalog, pokazuje vatrogasca koji zadobija povrede prilikom evakuacije zgrade, ne može se reći da je taj vatrogasac očigledno objavio svoje podatke. S druge strane, ako taj vatrogasac odluči da opiše događaj i objavi video-zapis i fotografije putem javne internet stranice, morao bi da preduzme svestan, potvrdan čin kako bi objavio lične podatke. Važno je napomenuti da objava sopstvenih podataka ne predstavlja pristanak, nego još jedno dopuštenje za obradu posebnih kategorija podataka.

Činjenica da je ispitanik objavio obrađene lične podatke ne oslobađa rukovaoce podacima njihovih obaveza na osnovu zakonodavstva o zaštiti podataka. Na primer, načelo ograničenja svrhe primenjuje se na lične podatke čak i ako takvi podaci postanu javno dostupni[424].

Pravni zahtevi

Obrada posebnih kategorija podataka koja je „nužna za uspostavu, ostvarivanje ili odbranu pravnih zahteva", nezavisno od toga da li se radi o parničnom postupku, upravnom ili vanparničnom postupku[425], takođe je dopuštena OUZP-om[426]. U tom

423 *Ibid.*, član 9. stav 2. tačka (d).

424 Radna grupa iz člana 29. (2013), *Opinion 3/2013 on purpose limitation* (Mišljenje 3/2013 o ograničavanju svrhe), WP 203, Bruxelles, 2. aprila 2013, str. 14.

425 Opšta uredba o zaštiti podataka, preambula, uvodna izjava 52.

426 *Ibid.*, član 9. stav 2. tačka (f).

slučaju, obrada mora biti relevantna za pojedini pravni zahtev, odnosno njegovo ostvarivanje ili odbranu, a može da je zatraži bilo koja od strana u sporu.

Kad sudovi deluju u sudskom svojstvu, mogu da obrađuju posebne kategorije podataka u kontekstu rešavanja pravnog spora[427]. Te posebne kategorije podataka koji se obrađuju u ovom kontekstu mogu uključivati, na primer, genetske podatke prilikom utvrđivanja roditeljstva ili zdravstveno stanje kada se deo dokaza odnosi na pojedinosti o povredama koje je zadobila žrtva krivičnog dela.

Razlozi značajnog javnog interesa

Prema članu 9. stav. 2 tačka (g) OUZP-a, države članice mogu propisati dodatne okolnosti u kojima osetljivi podaci mogu da se obrađuju:

- ako je obrada podataka potrebna zbog značajnog javnog interesa,
- ako je to propisano evropskim ili domaćim pravom,
- ako je evropsko ili domaće pravo srazmerno tako da se njime poštuje pravo na zaštitu podataka i obezbeđuju prikladne i posebne mere za zaštitu prava i interesa ispitanika[428].

Dobar primer su elektronski sistemi zdravstvenih kartona. Takvi sistemi omogućavaju dostupnost zdravstvenih podataka, koje prikupljaju zdravstveni radnici tokom lečenja pacijenta, drugim zdravstvenim radnicima tog pacijenta na širokoj osnovi, najčešće nacionalnoj.

Radna grupa iz člana 29. zaključila je da do uspostave takvih sistema ne bi moglo doći prema postojećim zakonskim propisima za obradu podataka o pacijentima[429]. Međutim, elektronski sistemi zdravstvenih kartona mogu postojati ako se zasnivaju na „potrebama značajnog javnog interesa"[430]. Za njihovu uspostavu bila bi potrebna

427 *Ibid*.

428 *Ibid*., član 9. stav 2. tačka (g).

429 Radna grupa iz člana 29. (2007), *Working Document on the processing of personal data relating to health in electronic health records (EHR)* (Radni dokument o obradi ličnih podataka koji se odnose na zdravlje u elektronskim zdravstvenim kartonima), WP 131, Bruxelles, 15. februara 2007. Videti i Opštu uredbu o zaštiti podataka, član 9. stav 3.

430 Opšta uredba o zaštiti podataka, član 9. stav 2. tačka (g).

izričita pravna osnova, koja bi uključivala i potrebne zaštitne mere za siguran rad sistema[431].

Ostale osnove za obradu osetljivih podataka

OUZP-om se propisuje da se osetljivi podaci mogu obrađivati ako je obrada nužna u svrhu[432]:

- preventivne medicine ili medicine rada radi procene radne sposobnosti zaposlenih, medicinske dijagnoze, pružanja zdravstvene ili socijalne pomoći ili tretmana ili upravljanja zdravstvenim ili socijalnim sistemima i uslugama na osnovu prava EU ili prava države članice ili u skladu sa ugovorom sa zdravstvenim radnikom,

- javnog interesa u oblasti javnog zdravlja kao što je zaštita od ozbiljnih prekograničnih pretnji zdravlju ili obezbeđivanje visokih standarda kvaliteta i sigurnosti zdravstvene zaštite kao i lekova i medicinskih proizvoda, na osnovu prava EU ili prava države članice. Pravom se moraju propisati odgovarajuće i posebne mere za zaštitu prava ispitanika,

- arhiviranja, naučnog ili istorijskog istraživanja ili u statističke svrhe na osnovu prava EU ili prava države članice. Pravo mora biti srazmerno cilju koji nastoji da se postigne, njime moraju da se poštuju suština prava na zaštitu podataka i obezbede prikladne i posebne mere za zaštitu prava i interesa ispitanika.

Dodatni uslovi na osnovu domaćeg zakonodavstva

OUZP-om se državama članicama takođe omogućava da uvedu ili zadrže dodatne uslove, uključujući ograničenja obrade genetskih podataka, biometrijskih podataka ili podataka koji se odnose na zdravlje[433].

431 Radna grupa iz člana 29. (2007), *Working Document on the processing of personal data relating to health in electronic health records (EHR)* (Radni dokument o obradi ličnih podataka koji se odnose na zdravlje u elektronskim zdravstvenim kartonima), WP 131, Bruxelles, 15. februara 2007.

432 Opšta uredba o zaštiti podataka, član 9. stav 2. tačke (h), (i) i (j).

433 *Ibid*., član 9. stav 2. tačka (h) i član 9. stav 4.

4.2. Pravila bezbednosti obrade

Ključne tačke

- Prema pravilima bezbednosti obrade, rukovalac podacima i obrađivač podataka obavezni su da sprovedu odgovarajuće tehničke i organizacione mere kako bi sprečili neovlašćeno ometanje postupaka obrade podataka.
- Neophodan nivo bezbednosti podataka određuje se prema:
  - bezbednosnim osobinama dostupnim na tržištu za određenu vrstu obrade,
  - troškovima,
  - rizicima obrade podataka za osnovna prava i slobode ispitanika.
- Obezbeđivanje poverljivosti ličnih podataka je deo opštih načela priznatih Opštom uredbom o zaštiti podataka.

Prema **pravu EU i Saveta Evrope**, rukovaoci podacima imaju opštu obavezu transparentnosti i odgovornosti pri obradi ličnih podataka, a posebno u pogledu povreda podataka kada do njih dođe. U slučaju povreda ličnih podataka, rukovaoci podacima moraju da izveste nadzorne organe, osim ako nije verovatno da će povreda ličnih podataka prouzrokovati rizik za prava i slobode pojedinaca. Ispitanici takođe treba da budu obavešteni o povredi ličnih podataka kada će ona verovatno dovesti do visokog rizika za prava i slobode pojedinaca.

4.2.1. Elementi bezbednosti podataka

Prema odgovarajućim odredbama **prava EU**:

> *„Uzimajući u obzir najnovija dostignuća, troškove sprovođenja kao i prirodu, opseg, kontekst i svrhe obrade, kao i rizik različitih nivoa verovatnoće i ozbiljnosti za prava i slobode pojedinaca, rukovalac podacima i obrađivač podataka sprovode odgovarajuće tehničke i organizacione mere kako bi obezbedili odgovarajući nivo bezbednosti s obzirom na rizik […].“*[434]

434 *Ibid.*, član 32. stav 1.

Te mere, između ostalog, uključuju sledeće:

- pseudonimizaciju i enkripciju ličnih podataka[435],
- obezbeđenje trajne poverljivosti, celovitosti, dostupnosti i otpornosti sistema i usluga obrade[436],
- pravovremeno ponovno uspostavljanje dostupnosti ličnih podataka i pristupa njima u slučaju gubitka podataka[437],
- proces za testiranje, ocenjivanje i procenjivanje delotvornosti mera za obezbeđivanje sigurnosti obrade[438].

Unutar **prava Saveta Evrope** postoji slična odredba:

> *„Svaka strana obezbeđuje da rukovalac podacima i, kada je to primenjivo, obrađivač podataka, preduzimaju odgovarajuće sigurnosne mere protiv rizika kao što su slučajno ili neovlašćeno uništenje, gubitak, upotreba, izmena ili otkrivanje ličnih podataka ili pristup njima."*[439]

Prema **pravu EU i Saveta Evrope**, u slučaju povrede podataka koja može uticati na prava i slobode pojedinaca, rukovalac podacima je dužan da o njoj obavesti nadzorni organ (videti deo 4.2.3).

Često su utvrđeni i industrijski, domaći i međunarodni standardi bezbedne obrade podataka. Na primer, Evropski pečat za zaštitu podataka (EuroPriSe) jeste projekat transevropske telekomunikacione mreže (eTEN) Evropske unije kojim se istražuju mogućnosti sertifikovanja proizvoda, naročito softvera, u svrhu usklađivanja s evropskim zakonodavstvom o zaštiti podataka. Agencija Evropske unije za mrežnu i informacionu bezbednost (ENISA) osnovana je radi unapređivanja sposobnosti Evropske unije, država članica Evropske unije i poslovne zajednice u pogledu sprečavanja, rešavanja i odgovaranja na probleme sa mrežnom i informacionom

435 *Ibid*., član 32. stav 1. tačka (a).
436 *Ibid*., član 32. stav 1. tačka (b).
437 *Ibid*., član 32. stav 1. tačka (c).
438 *Ibid*., član 32. stav 1. tačka (d).
439 Modernizovana Konvencija br. 108, član 7. stav 1.

sigurnošću[440]. ENISA redovno izdaje analize trenutnih sigurnosnih pretnji i savete o njihovom rešavanju[441].

Sigurnost podataka ne postiže se samo primenom prave opreme, odnosno hardvera i softvera. Ona zavisi i od odgovarajućih internih organizacijskih pravila. Takvim internim pravilima idealno bi bila obuhvaćena sledeća pitanja:

- redovno pružanje informacija svim zaposlenima o pravilima sigurnosti podataka i njihovim obavezama prema pravu zaštite podataka, naročito u pogledu njihovih obaveza poverljivosti,
- jasna raspodela odgovornosti i jasan prikaz stručnih veština u oblasti obrade podataka, naročito u pogledu odluka o obradi ličnih podataka i prenosa podataka trećim stranama ili ispitanicima,
- upotreba podataka samo prema uputstvima nadležne osobe ili prema generalno utvrđenim pravilima,
- zaštita pristupa lokacijama i hardveru i softveru rukovaoca podacima ili obrađivača podataka, uključujući provere ovlašćenja za pristup,
- obezbeđivanje da je ovlašćenja za pristup ličnim podacima dodelilo nadležno lice i zahtevanje odgovarajuće dokumentacije,
- automatizovani protokoli o pristupu ličnim podacima elektronskim putem i redovne provere takvih protokola koje vrši interna nadzorna služba (zbog čega je nužno da sve aktivnosti obrade podataka budu evidentirane),
- pažljivo dokumentovanje drugih oblika otkrivanja osim automatizovanog pristupa podacima kako bi se moglo dokazati da nije došlo ni do kakvih nezakonitih prenosa podataka.

440 Uredba (EZ) br. 526/2013 Evropskog parlamenta i Saveta od 21. maja 2013. o Agenciji Evropske unije za mrežnu i informacionu bezbednost (ENISA) i o stavljanju izvan snage Uredbe (EZ) br. 460/2004, SL 2013 L 165.

441 Na primer, ENISA, (2016.), *Cyber Security and Resilience of smart cars. Good practices and recommendations* (Sajbersigurnost i otpornost pametnih automobila: dobre prakse i preporuke); ENISA (2016.), *Security of Mobile Payments and Digital Wallets* (Sigurnost mobilnog plaćanja i digitalnih novčanika).

Ponuda odgovarajuće obuke i obrazovanja o bezbednosti podataka članovima osoblja takođe je važan elemenat delotvornih bezbednosnih mera opreza. Takođe je potrebno uspostaviti postupke provere kako bi se obezbedilo da odgovarajuće mere ne postoje samo na papiru, nego da se sprovode i deluju i u praksi (kao što su unutarnje ili spoljašnje revizije).

Mere za poboljšanje nivoa sigurnosti rukovaoca podacima ili obrađivača podataka uključuju instrumente kao što su službenici za zaštitu ličnih podataka, obuka zaposlenih o bezbednosti, redovne revizije, ispitivanja probojnosti i pečati kvaliteta.

> Primer: U predmetu *I. protiv Finske*[442] podnositeljka predstavke nije uspela da dokaže da su drugi zaposleni u bolnici u kojoj je radila nezakonito pristupili njenom zdravstvenom kartonu. Stoga su domaći sudovi odbacili njenu tužbu zbog povrede prava na zaštitu podataka. ESLJP je zaključio da je došlo do povrede člana 8. EKLJP-a jer bolnički sistem evidencije zdravstvenih kartona „nije omogućio retroaktivno obrazloženje upotrebe pacijentovih kartona s obzirom na to da je prikazivao samo pet poslednjih uvida i da su se te informacije brisale posle vraćanja datoteke u arhivu". Za ESLJP je od presudne važnosti bilo da bolnički evidencioni sistem očigledno nije bio u skladu sa zakonskim zahtevima iz domaćeg zakonodavstva, čemu domaći sudovi nisu pridali dovoljno važnosti.

Evropska unija donela je Direktivu o bezbednosti mrežnih i informacionih sistema (NIS direktiva)[443], prvi pravni instrument posvećen kibernetičkoj sigurnosti na nivou EU. Direktivom se nastoji da se poboljša kibernetička sigurnost na domaćem nivou i da se poveća nivo saradnje unutar EU. Njome se takođe propisuju obaveze za operatore ključnih usluga (uključujući operatore u energetskom, zdravstvenom, bankarskom i saobraćajnom sektoru, kao i u sektoru digitalne infrastrukture) i pružaoce digitalnih usluga koje se odnose na upravljanje rizicima, obezbeđenje sigurnosti njihovih mrežnih i informacionih sistema i prijavu sigurnosnih incidenata.

Mogućnosti

U septembru 2017. godine Evropska komisija izradila je predlog uredbe za reformu ovlašćenja ENISA-e kako bi se u obzir uzele nova ovlašćenja i odgovornosti te

442 ESLJP, *I. protiv Finske*, br. 20511/03, 17. jula 2008.

443 Direktiva (EU) 2016/1148 Evropskog parlamenta i Saveta od 6. jula 2016. o merama za visoki zajednički nivo bezbednosti mrežnih i informacionih sistema širom Unije, SL 2016 L 194.

agencije na osnovu NIS direktive. Cilj je predlog uredbe za razvijanje ENISA-inih zadataka i potvrda njene uloge „referentne tačke u sajberekosistemu EU-a"[444]. Predlogom uredbe ne smeju se dovesti u pitanje načela OUZP-a, a pojašnjavanjem nužnih elemenata koji čine evropske programe sajbersigurnosne sertifikate trebalo bi da se poveća bezbednost ličnih podataka. Istovremeno, u septembru 2017. Evropska komisija izradila je predlog implementacione uredbe kojom bi se utvrdili elementi koje pružaoci digitalnih usluga moraju uzeti u obzir kako bi zagarantovali bezbednost svojih mrežnih i informacionih sistema, kao što je propisano članom 16. stav 8. Direktive o NIS-u. U vreme izrade ovog priručnika, rasprave o ta dva predloga još su bile u toku.

4.2.2. Poverljivost

Unutar prava EU, OUZP-om se poverljivost ličnih podataka utvrđuje kao deo opšteg načela[445]. Pružaoci javno dostupnih elektronskih komunikacionih usluga moraju da obezbede poverljivost. Takođe imaju obavezu da garantuju sigurnost svojih usluga[446].

Primer: Zaposleni osiguravajućeg društva na poslu primi telefonski poziv od osobe koja tvrdi da je klijent i traži podatke o svom ugovoru o osiguranju.

S obzirom na to da je dužan da podatke klijenata čuva u tajnosti, zaposleni mora da primeni barem minimalne mere bezbednosti pre otkrivanja ličnih podataka. Način na koji to može da učini jeste, na primer, tako da ponudi da uzvrati poziv na telefonski broj zabeležen u klijentovom dosijeu.

Prema članu 5. stav 1. tačka (f), lični podaci moraju da se obrađuju na način kojim se obezbeđuje odgovarajuća sigurnost ličnih podataka, uključujući zaštitu od neovlašćene ili nezakonite obrade, kao i od slučajnog gubitka, uništenja ili oštećenja primenom odgovarajućih tehničkih ili organizacionih mera („celovitost i poverljivost").

U skladu sa članom 32., rukovalac podacima i obrađivač podataka moraju da sprovedu tehničke i organizacione mere za obezbeđivanje visokog nivoa sigurnosti.

444 Predlog uredbe Evropskog parlamenta i Saveta o ENISA-i (agenciji EU-a za sajbersigurnost) i stavljanju izvan snage Uredbe (EU) 526/2013 i o sajbersigurnosnoj sertifikaciji u oblasti informacione i komunikacione tehnologije („Akt o sajbersigurnosti"), COM(2017)477, 13. septembra 2017, str. 6.

445 Opšta uredba o zaštiti podataka, član 5. stav 1. tačka (f).

446 Direktiva o privatnosti i elektronskim komunikacijama, član 5. stav 1.

Takve mere između ostalog uključuju pseudonimizaciju i enkripciju ličnih podataka, sposobnost obezbeđivanja trajne poverljivosti, celovitosti, dostupnosti i otpornosti obrade, ocenjivanje i testiranje efikasnosti mera kao i sposobnost ponovne uspostave obrade podataka u slučaju fizičkog ili tehničkog incidenta. Osim toga, poštovanje odobrenog kodeksa ponašanja ili odobrenog mehanizma sertifikovanja može se iskoristiti kao elemenat za dokazivanje usklađenosti sa načelom celovitosti i poverljivosti. Prema članu 28. OUZP-a, ugovorom kojim se obrađivač podataka obavezuje prema rukovaocu podacima mora se odrediti da obrađivač podataka obezbeđuje da se osobe ovlašćene za obradu ličnih podataka obavežu na poštovanje poverljivosti ili da podležu primenjivim zakonskim obavezama o poverljivosti.

Obaveza poverljivosti ne odnosi se na situacije u kojima osoba sazna za podatke u svojstvu privatnog pojedinca, a ne zaposlenog rukovaoca podacima ili obrađivača podataka. U tom slučaju članovi 32. i 28. OUZP-a se ne primenjuju, jer je upotreba ličnih podataka koju sprovode privatni pojedinci potpuno izuzeta iz oblasti primene Uredbe kada takva upotreba potpada u okvire takozvanog izuzeća za domaćinstvo[447]. Izuzeće za domaćinstvo odnosi se na upotrebu ličnih podataka „koju sprovodi fizičko lice tokom isključivo ličnih ili kućnih aktivnosti"[448]. Posle odluke SPEU u predmetu *Bodil Lindqvist*[449] to izuzeće, međutim, treba usko tumačiti, naročito u pogledu otkrivanja podataka. Tačnije, izuzeće za domaću upotrebu ne proširuje se na objavu ličnih podataka neograničenom broju primalaca na internetu, niti na obradu podataka koja ima profesionalne ili komercijalne aspekte (za više pojedinosti o predmetu videti delove 2.1.2, 2.2.2. i 2.3.1).

„Poverljivost komunikacija" je još jedan aspekt poverljivosti, koji podleže *lex specialis*-u. Posebnim propisima za obezbeđivanje poverljivosti elektronskih komunikacija na osnovu Direktive o privatnosti i elektronskim komunikacijama državama članicama nalaže se da zabrane svim osobama koje nisu korisnici slušanje, prisluškivanje, čuvanje ili druge oblike presretanja, odnosno nadzora nad komunikacijama i metapodacima koji su s tim povezani, bez pristanka korisnika[450]. Domaćim zakonodavstvom mogu se dozvoliti izuzeća od tog načela isključivo kada je to nužno za nacionalnu bezbednost, odbranu, sprečavanje ili otkrivanje krivičnih dela, i samo ako su takve mere nužne i srazmerne ciljevima koji nastoje da se postignu[451]. Isti

447 Opšta uredba o zaštiti podataka, član 2. stav 2. tačka (c).

448 *Ibid.*

449 SPEU, C-101/01, *Krivični postupak protiv Bodil Lindqvist*, 6. novembra 2003.

450 Direktiva o privatnosti i elektronskim komunikacijama, član 5. stav 1.

451 *Ibid.*, član 15. stav 1.

propisi će se primenjivati u sklopu buduće Uredbe o e-privatnosti, ali oblast primene pravnog akta o e-privatnosti proširiće se s javno dostupnih elektronskih komunikacionih usluga na komunikacije putem „OTT usluga" (kao što su mobilne aplikacije).

Unutar prava Saveta Evrope obaveza poverljivosti podrazumeva se u pojmu bezbednosti podataka iz člana 7. stav 1. modernizovane Konvencije br. 108 u kome se obrađuje bezbednost podataka.

Za obrađivače podataka poverljivost znači da podatke ne smeju da otkrivaju trećim stranama, niti drugim primaocima bez ovlašćenja. Za službenike rukovaoca podacima ili obrađivača podataka poverljivosti znači da lične podatke smeju da upotrebljavaju samo u skladu s uputstvima svojih nadležnih nadređenih osoba.

Obaveza poverljivosti mora biti sadržana u svakom ugovoru između rukovalaca podacima i njihovih obrađivača podataka. Usto, rukovaoci podacima i obrađivači podataka moraju da preduzmu posebne mere kako bi za svoje zaposlene uspostavili pravnu obavezu poverljivosti. To se obično postiže uključivanjem odredbi o poverljivosti u ugovor o radu sa zaposlenim.

Kršenje profesionalne obaveze poverljivosti kažnjivo je na osnovu krivičnog prava u mnogim državama članicama EU i ugovornicama Konvencije br. 108.

4.2.3. Obaveštavanje u slučaju povrede ličnih podataka

Povreda/ugrožavanje ličnih podataka odnosi se na povredu bezbednosti koja dovodi do nehotičnog ili nezakonitog uništenja, gubitka, izmene ili neovlašćenog otkrivanja obrađenih ličnih podataka ili pristupa njima[452]. Iako nove tehnologije poput šifrovanja sada pružaju više mogućnosti za obezbeđivanje sigurnosti obrade, povrede podataka i dalje su česta pojava. Uzroci povreda podataka mogu biti razni, od nehotičnih pogrešaka koje počine osobe koje rade unutar organizacije do spoljašnjih pretnji kao što su hakeri i organizacije koje se bave sajberkriminalom.

Povrede podataka mogu da budu vrlo štetne za prava na privatnost i zaštitu podataka pojedinaca koji zbog takve povrede mogu izgubiti kontrolu nad svojim ličnim

452 Opšta uredba o zaštiti podataka, član 4. stav 12.; videti i *Smernice o obaveštavanju o povredi ličnih podataka na osnovu Uredbe 2016/679,* Radne grupe iz člana 29. (2017), WP 250, 3. oktobra 2017, str. 8.

podacima. Povrede podataka mogu dovesti do krađe identiteta ili prevare, finansijskog gubitka ili materijalne štete, gubitka poverljivosti ličnih podataka koji su zaštićeni poslovnom tajnom, kao i narušavanja ugleda ispitanika. U Smernicama o obaveštavanju o povredi ličnih podataka na osnovu Uredbe 2016/679 Radna grupa iz člana 29. objašnjava da povrede/ugrožavanje podataka mogu imati tri različite posledice za lične podatke: otkrivanje, gubitak i/ili izmenu[453]. Uz obavezu preduzimanja mera za obezbeđivanje sigurnosti obrade, kako je objašnjeno u delu 4.2, podjednako je važno osigurati da rukovaoci podacima u slučaju povrede podataka postupaju na odgovarajući način i pravovremeno.

Nadzorna tela i pojedinci često nisu svesni ugrožavanja podataka, zbog čega pojedinci ne mogu preduzeti potrebne korake da se zaštite od njenih negativnih posledica. Kako bi se potvrdila prava pojedinaca i ograničile posledice povreda podataka, **EU i Savet Evrope** u određenim okolnostima rukovaocima podacima nalažu obavezu obaveštavanja.

Prema modernizovanoj Konvenciji br. 108 **Saveta Evrope**, ugovorne strane moraju od rukovaoca podacima zahtevati barem da obaveste nadležno nadzorno telo o ugrožavanju podataka koje mogu ozbiljno da ometaju prava ispitanika. Takvo obaveštavanje mora se sprovesti „bez odlaganja"[454].

Pravom EU utvrđuje se detaljan režim rokova i sadržaja obaveštenja[455]. Rukovaoci podacima moraju da obaveste nadzorne organe o određenim povredama podataka bez nepotrebnog odlaganja i, ako je izvodljivo, najkasnije 72 sata posle saznanja o toj povredi. Ako se prekorači rok od 72 sata, obaveštavanje mora biti popraćeno obrazloženjem kašnjenja. Rukovaoci podacima izuzeti su od obaveze obaveštavanja samo ako mogu da dokažu da nije verovatno da će povreda podataka prouzrokovati rizik za prava i slobode dotičnih pojedinaca.

Uredbom se utvrđuju minimalne informacije koje moraju biti uključene u obaveštenje kako bi nadzorni organ mogao da preduzme potrebne mere.[456] Obaveštenje mora da sadrži barem opis prirode povrede podataka i kategorije i približan broj dotičnih ispitanika, opis verovatnih posledica povrede, kao i mere koje je rukovalac

453 Radna grupa iz člana 29. (2017), *Smernice o obaveštavanju o povredi ličnih podataka na osnovu Uredbe 2016/679*, WP 250, 3. oktobra 2017, str. 6.

454 Modernizovana Konvencija br. 108, član 7. stav 2.; Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, st. od 64 do 66.

455 Opšta uredba o zaštiti podataka, čl. 33. i 34.

456 *Ibid*., član 33. stav 3.

podacima preduzeo za rešavanje problema povrede i umanjivanje njenih posledica. Usto je potrebno navesti ime i kontakt podatke službenika za zaštitu podataka ili druge kontakt tačke kako bi nadležni nadzorni organ po potrebi mogao da dobije više informacija.

U slučaju povrede podataka koja će verovatno prouzrokovati visok rizik za prava i slobode pojedinaca, rukovalac podacima bez nepotrebnog odlaganja mora da obavesti pojedince (ispitanike) o povredi[457]. Informacije date ispitanicima, uključujući opis povrede podataka, moraju da budu napisane jasnim i jednostavnim jezikom i da uključuju informacije slične onima koje su nužne pri obaveštavanju nadzornih organa. U određenim okolnostima rukovaoci podacima mogu da budu izuzeti od obaveze obaveštavanja ispitanika o takvim povredama podataka. Izuzeća se primenjuju kada je rukovalac podacima preduzeo odgovarajuće tehničke i organizacione mere zaštite i te mere su primenjene na lične podatke zahvaćene povredom ličnih podataka, posebno one koje lične podatke čine nerazumljivima bilo kojoj osobi koja nije ovlašćena da im pristupi, kao što je enkripcija. Rukovalac podacima može da bude oslobođen obaveze obaveštavanja ispitanika i ako preduzme mere nakon povrede kako bi obezbedio da više ne dođe do visokog rizika za prava i slobode ispitanika. Na kraju, ako obaveštavanje zahteva nesrazmeran napor za rukovaoca podacima, ispitanici se mogu obavestiti o povredi podataka i na druge načine, poput javnog obaveštavanja ili sličnih mera[458].

Obaveza obaveštavanja nadzornih organa i ispitanika o povredama podataka odnosi se na rukovaoce podacima. Međutim, povrede podataka mogu se dogoditi nezavisno od toga da li obradu vrši rukovalac podacima ili obrađivač podataka. Zbog toga je neophodno obezbediti da obrađivači podataka takođe izveštavaju o povredama podataka. U tom slučaju obrađivači podataka moraju da obaveste rukovaoca podacima o povredama podataka bez nepotrebnog odlaganja[459]. Rukovalac podacima zatim je odgovoran za obaveštavanje nadzornih organa i dotičnih ispitanika u skladu sa prethodno navedenim pravilima i rokovima.

457 *Ibid.*, član 34.

458 *Ibid.*, član 34. stav 3. tačka (c).

459 *Ibid.*, član 33. stav 2.

4.3. Propisi o odgovornosti i unapređenju usklađenosti

Ključne tačke

- Kako bi se obezbedila odgovornost pri obradi ličnih podataka, rukovaoci podacima i obrađivači podataka moraju voditi evidenciju o aktivnostima obrade koje se obavljaju pod njihovom odgovornošću i na zahtev je pokazati nadzornim organima.
- U Opštoj uredbi o zaštiti podataka utvrđuje se nekoliko instrumenata za postizanje usklađenosti:
  - imenovanje službenika za zaštitu podataka u određenim slučajevima,
  - vršenje procene učinka pre početka aktivnosti obrade koje će verovatno prouzrokovati visok rizik za prava i slobode pojedinaca,
  - prethodno savetovanje s nadležnim nadzornim telom ako procena učinka ukazuje na to da obrada donosi rizike koji se ne mogu umanjiti,
  - kodeksi ponašanja za rukovaoce podacima i obrađivače podataka kojima se utvrđuje primena Uredbe u pojedinim sektorima obrade,
  - mehanizmi sertifikovanja, pečati i oznake.
- U sklopu prava Saveta Evrope, odnosno modernizovane Konvencije br. 108, predlažu se slični instrumenti za postizanje usklađenosti.

Načelo odgovornosti posebno je važno za obezbeđivanje sprovođenja propisa o zaštiti podataka u Evropi. Rukovalac podacima je odgovoran za usklađenost s propisima o zaštiti podataka i mora da bude u mogućnosti da je dokaže. Odgovornost ne bi smela da bude u prvom planu tek posle kršenja propisa. Naprotiv, rukovaoci podacima imaju proaktivnu obavezu da se pridržavaju odgovarajućih pravila za upravljanje podacima u svim fazama obrade podataka. Evropskim pravom zaštite podataka rukovaoci podacima obavezuju se na sprovođenje tehničkih i organizacionih mera kojima će obezbediti da se obrada sprovodi u skladu sa zakonom i dokazati tu usklađenost. Među tim merama su imenovanje službenika za zaštitu podataka, vođenje evidencije i dokumentacije u vezi s obradom i sprovođenje procena efekta na privatnost.

4.3.1. Službenici za zaštitu podataka

Službenici za zaštitu podataka (SZP) su lica koja daju savete o usklađenosti s propisima o zaštiti podataka u organizacijama koje vrše obradu podataka. Oni su „temelj odgovornosti" budući da doprinose usklađenosti i istovremeno deluju kao posrednici između nadzornih organa, ispitanika i organizacija koje ih imenuju.

Prema pravu Saveta Evrope, članom 10. stav 1. modernizovane Konvencije br. 108 rukovaocima podacima i obrađivačima podataka propisuje se opšta obaveza odgovornosti. Od rukovalaca podacima i obrađivača podataka zahteva se da preduzimaju sve odgovarajuće mere za usklađenost sa propisima o zaštiti podataka utvrđenim u Konvenciji, kao i da su u mogućnosti da dokažu da je obrada podataka pod njihovim vođstvom u skladu s odredbama Konvencije. Iako u Konvenciji nisu utvrđene konkretne mere koje rukovaoci podacima i obrađivači podataka treba da preduzmu, u Izveštaju sa objašnjenjima o modernizovanoj Konvenciji br. 108 navodi se da bi imenovanje SZP-a bila jedna od mogućih mera za dokazivanje usklađenosti. SZP-ovi na raspolaganju treba da imaju sva potrebna sredstva kako bi ispunili svoja ovlašćenja[460].

Za razliku od prava Saveta Evrope, **u EU** imenovanje SZP-a nije uvek prepušteno odluci rukovaoca podacima i obrađivača podataka, već je u određenim uslovima i obavezno. U OUZP-u se službenik za zaštitu podataka smatra ključnom ulogom u novom sistemu upravljanja, te se navode podrobne odredbe o imenovanju, funkciji, dužnostima i zadacima tog službenika[461].

Prema OUZP-u, imenovanje službenika za zaštitu podataka obavezno je u tri posebna slučaja: kada obradu vrši organ javne vlasti ili javni organ, kada se osnovne delatnosti rukovaoca ili obrađivača podataka sastoje od postupaka obrade koji iziskuju redovno i sistematsko praćenje ispitanika u velikoj razmeri ili kada se njihove osnovne delatnosti sastoje od opsežne obrade posebnih kategorija podataka ili ličnih podataka u vezi sa krivičnim osudama i krivičnim delima[462]. Iako pojmovi „sistematsko praćenje u velikoj razmeri" i „osnovne delatnosti" nisu definisani u Uredbi, Radna grupa iz člana 29. objavila je smernice o njihovom tumačenju[463].

460 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 87.

461 Opšta uredba o zaštiti podataka, čl. od 37. do 39.

462 *Ibid*., član 37. stav 1.

463 Radna grupa iz člana 29. (2017), *Smernice o službenicima za zaštitu podataka („SZP-ovima")*, WP 243 rev.01, poslednji put revidirane i donesene 5. aprila 2017.

Primer: Kompanije koja upravljaju društvenim mrežama i internet pretraživačima verovatno će se smatrati rukovaocima podacima čiji postupci obrade zahtevaju redovno i sistematsko praćenje ispitanika u velikoj razmeri. Poslovni model takvih kompanija zasniva se na obradi velikih količina ličnih podataka tako da one ostvaruju znatan prihod od pružanja ciljanih marketinških usluga i omogućavanja drugim kompanijama da se oglašavaju na njihovim internet stranicama. Ciljano oglašavanje odnosi se na postavljanje oglasa na osnovu demografije i ranijih kupovina ili ponašanja kupaca. Za njega je zato potrebno sistematično praćenje navika i ponašanja ispitanika na internetu.

Primer: Bolnica i osiguravajuće društvo tipični su primeri rukovaoca podacima čije se aktivnosti sastoje od opsežne obrade posebnih kategorija ličnih podataka. Podaci koji otkrivaju informacije o zdravlju osoba čine posebne kategorije ličnih podataka prema pravu Saveta Evrope i EU, pa zato zahtevaju pojačanu zaštitu. Prema pravu EU, genetski i biometrijski podaci takođe se smatraju posebnim kategorijama. Ako zdravstvene ustanove i osiguravajuća društva obrađuju takve podatke u velikoj razmeri, na osnovu OUZP-a dužni su da imenuju službenika za zaštitu podataka.

Usto, članom 37. stav 4. OUZP-a utvrđeno je da u slučajevima, osim tri obavezna iz člana 37. stav 1., rukovalac podacima, obrađivač podataka ili udruženja i druga tela koji predstavljaju kategoriju rukovaoca podacima ili obrađivača podataka mogu ili, ako to nalaže pravo Unije ili pravo države članice, moraju da imenuju službenika za zaštitu podataka.

Druge organizacije nisu zakonski obavezne da imenuju SZP-a. Međutim, OUZP-om je utvrđeno da rukovaoci podacima i obrađivači podataka mogu dobrovoljno da imenuju SZP-a tako da se istovremeno državama članicama omogućava da imenovanje službenika proglase obaveznim za više vrsta organizacija od onih navedenih u Uredbi[464].

Kada rukovalac podacima imenuje službenika za zaštitu podataka, mora obezbediti da je on „na primeren način i pravovremeno uključen u sva pitanja u pogledu zaštite ličnih podataka" unutar organizacije[465]. Na primer, SZP-ovi treba da budu uključeni u savetovanje o vršenju procena efekta zaštite podataka, kao i u izradu i vođenje

464 Opšta uredba o zaštiti podataka, član 37. st. 3 i 4.

465 *Ibid*., član 38. stav 1.

evidencije aktivnosti obrade u organizaciji. Kako bi SZP-ovi efikasno izvršavali svoje zadatke, rukovaoci podacima i obrađivači podataka moraju da im obezbede potrebne izvore, uključujući finansijska sredstva, infrastrukturu i opremu. Dodatni zahtevi uključuju davanje dovoljno vremena SZP-ovima kako bi ispunili svoje funkcije i redovnu obuku kako bi mogli da razvijaju svoje stručne veštine i prate razvoj zakonodavstva o zaštiti podataka[466].

OUZP-om se uspostavljaju određene osnovne garancije kojima se obezbeđuje da službenici za zaštitu podataka nezavisno deluju. Rukovaoci podacima i obrađivači podataka moraju obezbediti da u sprovođenju svojih zadataka povezanih sa zaštitom podataka SZP-ovi ne dobijaju nikakva uputstva od kompanije, kao ni od osoba na najvišim upravljačkim funkcijama. Usto, on ne sme da se razreši dužnosti, niti kazni zbog izvršavanja njegovih zadataka[467]. Na primer, u jednom slučaju SZP savetuje rukovaocu ili obrađivaču podataka da sprovede procenu efekta zaštite podataka jer smatra da će obrada verovatno prouzrokovati visok rizik za ispitanike. Kompanija se ne slaže sa savetom SZP-a jer ne smatra da je utemeljen, pa zato odlučuje da neće da sprovede procenu efekta. Kompanija može da zanemari savet, ali ne sme službenika da razreši dužnosti niti da ga kazni što ga je dao.

Zadaci i dužnosti SZP-a detaljno su opisani u članu 39. OUZP-a. Oni uključuju obavezno informisanje i savetovanje kompanija i zaposlenih koji obavljaju obradu o njihovim obavezama u skladu sa zakonodavstvom, kao i praćenje poštovanja propisa EU i domaćih propisa koji se odnose na zaštitu podataka putem revizija i osposobljavanja osoblja koje učestvuje u postupcima obrade. SZP-ovi takođe moraju da sarađuju s nadzornim telom i deluju kao kontakt tačka za nadzorno telo o pitanjima u pogledu obrade, kao što je povreda podataka.

Kad je reč o ličnim podacima kojima rukuju institucije i tela EU, Uredbom 45/2001 propisuje se da svaka institucija i telo Unije mora da imenuje SZP-a. SZP ima obavezu da obezbedi da se odredbe Uredbe pravilno sprovode u institucijama i telima EU, kao i da su i ispitanici i rukovaoci podacima obavešteni o svojim pravima i obavezama[468]. Taj službenik je takođe odgovoran za odgovaranje na zahteve Evropskog nadzornika za zaštitu podataka (EDPS) i, po potrebi, saradnju s njim. Slično kao i OUZP, Uredba 45/2001 sadrži odredbe o nezavisnosti SZP-ova u izvršavanju njihovih

466 Radna grupa iz člana 29. (2017), Smernice o službenicima za zaštitu podataka („SZP-ovima"), WP 243 rev.01, poslednji put revidirane i donesene 5. aprila 2017, tačka 3.1.

467 Opšta uredba o zaštiti podataka, član 38. st. 2 i 3.

468 Videti član 24. stav 1. Uredbe (EZ) br. 45/2001 za celovit popis zadataka službenika za zaštitu podataka.

zadataka i o potrebi za obezbeđenjem osoblja i sredstava koji su im potrebni[469]. SZP-ovi se moraju obavestiti pre nego što neka institucija ili telo EU (ili odseci tih organizacija) sprovede bilo koji postupak obrade i oni moraju da vode evidenciju svih prijavljenih postupaka obrade[470].

4.3.2. Evidencija aktivnosti obrade

Da bi mogle da dokažu usklađenost i preuzmu odgovornost, kompanije su često zakonski obavezane da dokumentuju i evidentiraju svoje aktivnosti. Važan primer su poreski zakoni i revizije, za koje je nužno da sve kompanije vode opsežnu dokumentaciju i evidenciju. Utvrđivanje sličnih zahteva u drugim područjima zakonodavstva, naročito zakonodavstva o zaštiti podataka, takođe je važno jer je vođenje evidencije važan način za postizanje usklađenosti s propisima o zaštiti podataka. **Pravom EU** stoga se propisuje da rukovaoci podacima ili njihovi predstavnici moraju voditi evidenciju aktivnosti obrade za koje su odgovorni[471]. Tom obavezom nastoji da se osigura da nadzorna tela po potrebi na raspolaganju imaju potrebnu dokumentaciju kako bi potvrdila zakonitost obrade podataka.

Informacije koje treba da se evidentiraju uključuju sledeće:

- ime i kontakt podatke rukovaoca podacima i, ako je primenjivo, zajedničkog rukovaoca podacima, predstavnika rukovaoca podacima i službenika za zaštitu podataka,
- svrhe obrade,
- opis kategorija ispitanika i kategorija ličnih podataka povezanih s obradom,
- informacije o kategorijama primalaca kojima su lični podaci otkriveni ili će biti otkriveni,
- informacije o tome da li su ili da li će lični podaci biti preneseni u treće zemlje ili međunarodne organizacije,
- ako je to moguće, predviđene rokove za brisanje različitih kategorija ličnih podataka i pregled tehničkih mera donesenih za obezbeđivanje sigurnosti obrade[472].

469 Uredba (EZ) br. 45/2001, član 24. st. 6. i 7.

470 *Ibid*., čl. 25 i 26.

471 Opšta uredba o zaštiti podataka, član 30.

472 *Ibid*., član 30. stav 1.

Obaveza vođenja evidencije aktivnosti obrade prema OUZP-u ne odnosi se samo na rukovaoca podacima nego i na obrađivače podataka. To je važna novost jer je pre donošenja Uredbe ugovor sklopljen između rukovaoca i obrađivača podataka prvenstveno obuhvatao obaveze obrađivača podataka. Njihova obaveza vođenja evidencije sada je neposredno predviđena zakonom.

OUZP-om se propisuje i izuzeće od te obaveze. Zahtev vođenja evidencije ne odnosi se na preduzeće ili organizaciju (rukovaoca i obrađivača podataka) koja ima manje od 250 zaposlenih. Međutim, to izuzeće podleže uslovima prema kojima dotična organizacija ne sme vršiti obradu koja će verovatno dovesti do rizika za prava i slobode ispitanika i prema kojima je obrada samo povremena i ne uključuje posebne kategorije podataka iz člana 9. stav 1., niti lične podatke u vezi sa krivičnim presudama i kažnjivim delima iz člana 10.

Vođenje evidencije o aktivnostima obrade trebalo bi omogućiti rukovaocima podacima i obrađivačima podataka da dokažu usklađenost s Uredbom. Takođe bi trebalo omogućiti nadzornim organima da prate zakonitost obrade podataka. Ako nadzorni organ zatraži pristup toj evidenciji, rukovaoci podacima i obrađivači podataka dužni su da sarađuju i stave je na raspolaganje.

4.3.3. Procena efekta zaštite podataka i prethodno savetovanje

Postupci obrade donose određene rizike za prava pojedinaca. Lični podaci se mogu izgubiti, otkriti neovlašćenim stranama ili obraditi na nezakonit način. Rizici se, naravno, razlikuju u zavisnosti od prirode i opsega obrade. Na primer, postupci većih razmera koji uključuju obradu osetljivih podataka donose mnogo veći rizik za ispitanike u odnosu na potencijalne rizike kada neka manja kompanija obrađuje adrese i lične telefonske brojeve svojih zaposlenih.

S pojavom novih tehnologija i sve složenijom obradom podataka, rukovaoci podacima moraju da otklone takve rizike uz pomoć procene verovatnog efekta predviđene obrade pre početka samog postupka obrade. Time se omogućava da organizacije pravilno prepoznaju, otklone i umanje rizike unapred i tako znatno ograniče verovatnoću negativnog efekta obrade na pojedince.

Procene efekta zaštite podataka predviđene su **pravom Saveta Evrope i EU**. Unutar pravnog okvira Saveta Evrope, članom 10. stav 2. modernizovane Konvencije br. 108 od ugovornih strana zahteva se da obezbede da rukovaoci podacima i obrađivači podataka „ispitaju verovatni učinak planirane obrade podataka na prava i osnovne

slobode ispitanika pre početka takve obrade" i da na osnovu te procene osmisle obradu tako da se spreče ili umanje rizici povezani s njom.

Pravom EU nameće se slična, ali detaljnija, obaveza rukovaocima podacima koji su obuhvaćeni područjem primene OUZP-a. Članom 35. utvrđuje se da se procena efekta mora sprovesti kada je verovatno da će obrada prouzrokovati visok rizik za prava i slobode pojedinaca. U Uredbi nije utvrđeno kako verovatnoća rizika treba da se proceni, nego se samo navodi koji su mogući rizici[473]. Naveden je popis postupaka obrade koji se smatraju visokorizičnima i za koje je prethodna procena efekta posebno važna. To su prvenstveno sledeći slučajevi:

- lični podaci obrađuju se radi donošenja odluka o pojedincima na osnovu bilo kakve sistemske i opsežne procene ličnih aspekata u vezi s pojedincima (izrada profila),
- osetljivi podaci ili lični podaci u vezi sa krivičnim presudama i krivičnim delima obrađuju se u većoj meri,
- obrada uključuje opsežno, sistemsko praćenje javno dostupnih oblasti.

Nadzorna tela moraju doneti i javno objaviti popis vrsta postupaka obrade koji podležu procenama efekta. Takođe mogu uspostaviti popis postupaka obrade koji su izuzeti iz te obaveze[474].

Kada je potrebna procena efekta, rukovaoci podacima moraju proceniti nužnost i srazmernost obrade i moguće rizike za prava pojedinaca. Procena efekta takođe mora uključivati planirane mere bezbednosti za otklanjanje utvrđenih rizika. Za uspostavljanje popisa nadzorna tela država članica moraju sarađivati međusobno i s Evropskim odborom za zaštitu podataka. Time će se obezbediti dosledan pristup na nivou EU za postupke u kojima je potrebna procena efekta, a rukovaocima podacima biće postavljeni slični zahtevi nezavisno od njihove lokacije.

473 Opšta uredba o zaštiti podataka, preambula, uvodna izjava 75.

474 *Ibid*., član 35. st. 4. i 5.

Ako se nakon procene efekta čini da će obrada dovesti do visokog rizika za prava pojedinaca, a nisu uvedene mere za umanjivanje tog rizika, rukovalac podacima se mora savetovati s nadležnim nadzornim telom pre početka postupka obrade[475].

Radna grupa iz člana 29. izdala je smernice o proceni efekta zaštite podataka i o tome kako utvrditi verovatnoću da će obrada dovesti do visokog rizika[476]. Grupa je razvila devet merila za utvrđivanje nužnosti procene efekta zaštite podataka u pojedinačnom slučaju[477]: (1) procena ili bodovanje; (2) automatizovano donošenje odluka s pravnim ili sličnim znatnim efektom; (3) sistemsko praćenje; (4) osetljivi podaci; (5) opsežna obrada podataka; (6) podudarajući ili kombinovani skupovi podataka; (7) podaci koji se odnose na osetljive ispitanike; (8) inovativna upotreba ili primena novih tehnoloških ili organizacionih rešenja; (9) situacija u kojoj sama obrada „sprečava ispitanike u ostvarivanju prava ili upotrebi usluge i ugovora". Radna grupa iz člana 29. uvela je korisno pravilo prema kojem postupci obrade koji ispunjavaju manje od dva kriterijuma predstavljaju niži rizik i ne zahtevaju procenu zaštite podataka, dok postupci koji ispunjavaju dva ili više kriterijuma zahtevaju procenu. Ako nije jasno da li je procena efekta zaštite podataka potrebna, Radna grupa iz člana 29. preporučuje da se ona ipak sprovede jer „rukovaocima podacima olakšava usklađivanje sa zakonodavstvom o zaštiti podataka"[478]. Važno je sprovesti procenu efekta zaštite podataka pri uvođenju nove tehnologije za obradu podataka[479].

4.3.4. Kodeksi ponašanja

Kodeksi ponašanja namenjeni su upotrebi u nekoliko industrijskih sektora kako bi se opisala i utvrdila primena OUZP-a u pojedinim sektorima. Rukovaocima podacima i obrađivačima podataka ličnih podataka izrada kodeksa može pomoći da znatno poboljšaju usklađenost i sprovođenje propisa o zaštiti podataka EU. Stručno znanje članova sektora pomoći će u pronalasku praktičnih rešenja za koje je moguće da će biti prihvaćena. Potvrđujući važnost takvih kodeksa u delotvornom sprovođenju zakonodavstva o zaštiti podataka, OUZP-om se države članice, nadzorna tela, Komisija i Evropski odbor za zaštitu podataka pozivaju da podstaknu izradu kodeksa

475 *Ibid.*, član 36. stav 1.; Radna grupa iz člana 29. (2017), *Smernice o proceni učinka na zaštitu podataka i utvrđivanje mogu li postupci obrade „verovatno da prouzrokuju visok rizik" u smislu Uredbe 2016/679*, WP 248 rev.01, Bruxelles, 4. oktobra 2017.

476 Radna grupa iz člana 29. (2017), *Smernice o proceni učinka na zaštitu podataka i utvrđivanje mogu li postupci obrade „verovatno da prouzrokuju visok rizik" u smislu Uredbe 2016/679*, WP 248 rev.01, Bruxelles, 4. oktobra 2017.

477 *Ibid*., str. 9–11.

478 *Ibid*., str. 9.

479 *Ibid*.

ponašanja koji su namenjeni unapređivanju pravilnog sprovođenja Uredbe na nivou EU[480]. Kodeksima se može utvrditi sprovođenje Uredbe u pojedinim sektorima, uključujući pitanja poput prikupljanja ličnih podataka, informacija koje treba da se daju ispitanicima i javnosti i ostvarivanja prava ispitanika.

Kako bi se obezbedilo da kodeksi ponašanja budu usklađeni s odredbama OUZP-a, oni se moraju podneti nadležnom nadzornom organu pre donošenja. Nadzorni organ daje mišljenje o tome da li je nacrt kodeksa u skladu s Uredbom i takav nacrt kodeksa odobrava ako smatra da obezbeđuje dovoljno prikladne zaštitne mere[481]. Nadzorni organi moraju da objave odobrene kodekse ponašanja kao i merila na kojima se odobrenje zasniva. Ako se nacrt kodeksa ponašanja odnosi na aktivnosti obrade u nekoliko država članica, nadležni nadzorni organ pre davanja odobrenja podnosi nacrt kodeksa, izmenu ili proširenje Evropskom odboru za zaštitu podataka koji daje mišljenje o usklađenosti kodeksa s OUZP-om. Komisija može implementornim aktima odlučiti da odobreni kodeks ponašanja koji joj je predat ima opštu valjanost unutar Unije.

Pridržavanjem kodeksa ponašanja ostvaruju se važne prednosti kako za ispitanike, tako i za rukovaoce podacima i obrađivače podataka. Takvi kodeksi pružaju detaljne smernice kojima se pravni zahtevi mogu prilagoditi pojedinim sektorima i kojima se podstiče transparentnost aktivnosti obrade podataka. Rukovaoci podacima i obrađivači podataka takođe mogu iskoristiti pridržavanje kodeksa kao jasan dokaz svoje usklađenosti s pravom EU i kao način poboljšanja svog javnog ugleda kao organizacija koje su predate zaštiti podataka u svom radu i stavljaju je na prvo mesto. Odobreni kodeksi ponašanja u kombinaciji s obavezujućim i sprovodljivim obavezama mogu se upotrebiti kao odgovarajuće zaštitne mere za prenos podataka u treće zemlje. Da bi se obezbedilo da organizacije koje se pridržavaju kodeksa ponašanja zaista i budu usklađene s njima, može se imenovati posebno telo (koje akreditуje nadležno nadzorno telo) radi praćenja i obezbeđivanja usklađenosti. Za efikasno ispunjavanje svojih zadataka to telo mora biti nezavisno, imati dokazanu stručnost u pitanjima koja su uređena kodeksom ponašanja i imati transparentne postupke i strukture za rešavanje pritužbi na kršenja kodeksa[482].

Prema **pravu Saveta Evrope**, modernizovanom Konvencijom br. 108 utvrđeno je da se nivo zaštite podataka koji je zagarantovan domaćim zakonodavstvom može

480 Opšta uredba o zaštiti podataka, član 40. stav 1.

481 *Ibid*., član 40. stav 5.

482 *Ibid*., član 41. st. 1 i 2.

korisno pojačati dobrovoljnim regulatornim merama, poput kodeksa dobre prakse ili kodeksa profesionalnog ponašanja. Međutim, to su isključivo dobrovoljne mere prema modernizovanoj Konvenciji br. 108: nije moguće uspostaviti nikakvu pravnu obavezu za uvođenje takvih mera, iako se to preporučuje, te takve mere same po sebi nisu dovoljne da bi se obezbedila potpuna usklađenost s Konvencijom[483].

4.3.5. Sertifikovanje

Uz kodekse ponašanja, mehanizmi sertifikovanja, kao i pečati i oznake zaštite podataka, su dodatno sredstvo pomoću kojeg rukovaoci podacima i obrađivači podataka mogu da dokažu svoju usklađenost s OUZP-om. U tu svrhu Uredbom se propisuje dobrovoljan sistem sertifikovanja putem kojeg određena tela ili nadzorna tela mogu izdavati sertifikate. Rukovaoci podacima i obrađivači podataka koji odluče da upotrebljavaju mehanizam sertifikovanja mogu ostvariti veću vidljivosti i verodostojnost, budući da sertifikati, pečati i oznake omogućavaju ispitanicima da brzo procene nivo zaštite pri obradi podataka pojedinih organizacija. Važno je napomenuti da činjenica da neki rukovalac ili obrađivač podataka ima sertifikat ne podrazumeva da su njegove dužnosti i odgovornosti nužno u skladu sa svim odredbama Uredbe.

4.4. Tehnička i integrisana zaštita podataka

Tehnička zaštita podataka

Pravom EU od rukovaoca podacima zahteva se uspostavljanje mera za efikasnu primenu načela zaštite podataka i uključenje potrebnih zaštitnih mera u obradu radi ispunjavanja zahteva iz Uredbe i zaštite prava ispitanika[484]. Te mere treba da se sprovode i u trenutku obrade i prilikom utvrđivanja sredstva obrade. Prilikom sprovođenja tih mera rukovalac podacima mora uzeti u obzir najnovija dostignuća, troškove sprovođenja, prirodu, opseg i svrhe obrade ličnih podataka kao i rizike i ozbiljnost za prava i slobode ispitanika[485].

Prema pravu Saveta Evrope od rukovaoca podacima i obrađivača podataka zahteva se da procene verovatan efekat obrade ličnih podataka na prava i slobode ispitanika

483 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 33.

484 Opšta uredba o zaštiti podataka, član 25. stav 1.

485 Vidi Radna grupa iz člana 29. (2017), *Smernice o proceni efekta na zaštitu podataka i utvrđivanje mogu li postupci obrade „verovatno da prouzrokuju visok rizik" u smislu Uredbe 2016/679*, WP 248 rev.01, 4. oktobra 2017. Videti i ENISA (2015.), *Privacy and Data Protection by Design-from policy to engineering* (Privatnost i tehnička zaštita podataka: od politike do projektovanja), 12. januara 2015.

pre početka same obrade. Usto, rukovaoci podacima i obrađivači podataka dužni su da organizuju obradu podataka tako da se spreči ili umanji rizik od mešanja u ta prava i slobode i da sprovedu tehničke i organizacione mere koje su osmišljene uzimajući u obzir aspekt prava na zaštitu ličnih podataka u svim fazama obrade podataka[486].

Integrisana zaštita podataka

Prema pravu EU od rukovaoca podacima se zahteva da sprovede odgovarajuće mere kako bi obezbedio da se integrisanim načinom obrađuju samo lični podaci koji su nužni za određenu svrhu. Ta obaveza se primenjuje na količinu prikupljenih ličnih podataka, opseg njihove obrade, period čuvanja i njihovu dostupnost[487]. Takvom merom se mora obezbediti, na primer, da nemaju svi službenici rukovaoca podacima pristup ličnim podacima lica čiji se podaci obrađuju. Dodatne smernice je razvio EDPS u *Paketu alata za određivanje nužnosti mera*[488].

Prema pravu Saveta Evrope od rukovaoca podacima i obrađivača podataka zahteva se da sprovedu tehničke i organizacione mere kako bi u obzir uzeli aspekt prava na zaštitu podataka, kao i da sprovedu tehničke i organizacione mere koje su osmišljene uzimajući u obzir aspekt prava na zaštitu podataka u svim fazama obrade podataka[489].

ENISA je 2016. objavila izveštaj o dostupnim alatima i uslugama za privatnost[490]. Između ostalog, ta procena uključuje pokazatelj merila i parametara koji predstavljaju pokazatelje dobrih odnosno loših praksi u vezi s privatnošću. Neka merila su neposredno povezana s odredbama OUZP-a, poput upotrebe pseudonimizacije i odobrenih mehanizama sertifikovanja, a drugima se pružaju inovativne inicijative za obezbeđivanje tehničke i integrisane privatnosti. Na primer, kriterijum upotrebljivosti može poslužiti za poboljšanje privatnosti, iako nije direktno s njom povezan, jer može omogućiti šire usvajanje alata ili usluge za privatnost. Šira javnost može

---

486 Modernizovana Konvencija br. 108, član 10. st. 2 i 3, Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 89.

487 Opšta uredba o zaštiti podataka, član 25. stav 2.

488 Evropski nadzornik za zaštitu podataka (EDPS) (2017.), *Necessity Toolkit* (Paket alata za određivanje nužnosti mera), Bruxelles, 11. aprila 2017.

489 Modernizovana Konvencija br. 108, član 10. stav 3., Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 89.

490 ENISA, *PETs controls matrix: A systematic approach for assessing online and mobile privacy tools* (Kontrolna matrica PET-ova: sistemski pristup za ocenjivanje alata za privatnost na mreži i u mobilnoj telefoniji), 20. decembra 2016.

u manjoj meri usvajati alate za privatnost koje je teže sprovesti u praksi, čak i ako pružaju snažnu zaštitu privatnosti. Usto, kriterijum razvijenosti i stabilnosti alata za privatnost, odnosno način na koji se alat razvija s vremenom i prilagođava postojećim ili novim izazovima u vezi s privatnošću, od ključne je važnosti. Druge tehnologije pojačane privatnosti, na primer, u kontekstu sigurnih komunikacija, uključuju šifrovanje „s kraja na kraj" (komunikaciju u kojoj isključivo osobe koje komuniciraju mogu čitati poruke); šifrovanje klijent-server (šifrovanje komunikacionog kanala koji se uspostavlja između klijenta i servera); autentifikaciju (proveru identiteta strana koje komuniciraju) i anonimnu komunikaciju (nijedna treća strana ne može identifikovati strane koje komuniciraju).

5 Nezavisni nadzor

EU	Obuhvaćena pitanja	Savet Evrope
Povelja (dostupna na engleskom jeziku), član 8. stav 3. Ugovor o funkcionisanju Evropske unije (dostupan na engleskom jeziku), član 16. stav 2. Opšta uredba o zaštiti podataka, članovi od 51. do 59. SPEU, C-518/07, *Evropska komisija protiv Savezne Republike Nemačke* [VV], 2010. SPEU, C-614/10, *Evropska komisija protiv Republike Austrije* [VV], 2012. SPEU, C-288/12, *Evropska komisija protiv Mađarske* [VV], 2014. SPEU, C-362/14, *Maximillian Schrems protiv Data Protection Commissioner* [VV], 2015.	**Nadzorna tela**	Modernizovana Konvencija br. 108, član 15.
Opšta uredba o zaštiti podataka, članovi od 60. do 67.	**Saradnja nadzornih tela**	Modernizovana Konvencija br. 108, članovi od 16. do 21.
Opšta uredba o zaštiti podataka, članovi od 68. do 76.	**Evropski odbor za zaštitu podataka**	

Ključne tačke

- Nezavisni nadzor je ključni element evropskog prava zaštite podataka i utvrđen je članom 8. stav 3. Povelje.
- Radi obezbeđenja delotvorne zaštite podataka, domaćim zakonodavstvom moraju biti uspostavljena nezavisna nadzorna tela.
- Nadzorna tela moraju delovati potpuno nezavisno, a nezavisnost im se mora garantovati pravom na osnovu kojeg su uspostavljena i mora se odražavati u posebnoj organizacionoj strukturi nadzornog tela.
- Nadzorna tela imaju posebna ovlašćenja i zadatke. Ona, između ostalog, uključuju sledeće:
  - nadzor i unapređenje zaštite podataka na domaćem nivou,
  - savetovanje ispitanika i rukovalaca podacima, kao i vlade i šire javnosti,
  - saslušanje prigovora i pomaganje ispitanicima u vezi sa navodnim kršenjem prava na zaštitu podataka,
  - nadzor rukovalaca podacima i obrađivača podataka.
- Nadzorna tela takođe imaju ovlašćenje da intervenišu po potrebi, i to:
  - upozoravanjem, opominjanjem ili čak novčanim kažnjavanjem rukovaoca podacima i obrađivača podataka izdavanjem naloga da se podaci isprave, blokiraju ili izbrišu,
  - nametanjem zabrane obrade ili upravne novčane kazne,
  - upućivanjem slučajeva sudu.
- Budući da obrada ličnih podataka često uključuje rukovaoce podacima i obrađivače podataka i ispitanike koji se nalaze u različitim državama, nadzorna tela moraju međusobno da sarađuju na prekograničnim pitanjima kako bi obezbedila delotvornu zaštitu pojedinaca u Evropi.
- Opštom uredbom o zaštiti podataka u EU se uspostavlja jedinstveni mehanizam za slučajeve prekogranične obrade. Neke kompanije obavljaju prekogranične aktivnosti obrade zbog obrade ličnih podataka u kontekstu aktivnosti sedišta u više od jedne države članice ili u kontekstu jedinog sedišta u Uniji, koji bitno utiče na ispitanike u više od jedne države članice. U skladu sa mehanizmom, takve kompanije moraju da sarađuju samo s jednim domaćim nadzornim telom za zaštitu podataka.
- Mehanizam saradnje i doslednosti omogućiće koordinisani pristup svih nadzornih tela koja učestvuju u slučaju. Vodeće nadzorno telo glavnog ili jedinog sedišta savetovaće se sa drugim nadležnim nadzornim telima i podneti im svoj nacrt odluke.

- Slično kao i trenutna Radna grupa iz člana 29., nadzorno telo svake države članice i Evropski nadzornik za zaštitu podataka (EDPS) biće članovi Evropskog odbora za zaštitu podataka.
- Zadaci Evropskog odbora za zaštitu podataka uključuju, na primer, praćenje pravilnog sprovođenja Uredbe, savetovanje Komisije o relevantnim pitanjima, kao i izdavanje mišljenja, smernica ili najboljih praksi o različitim temama.
- Osnovna razlika je to što Evropski odbor za zaštitu podataka neće samo izdavati mišljenja na osnovu Direktive 95/46/EZ. Takođe će donositi obavezujuće odluke o slučajevima u kojima nadzorno telo podnese relevantan i obrazložen prigovor na jedinstvene kontakt tačke, kada postoje oprečna mišljenja o tome koje je nadzorno telo vodeće i, na kraju, kada nadležno nadzorno telo ne zatraži ili ne uzme u obzir mišljenje Odbora. Cilj je da se obezbedi dosledno sprovođenje Uredbe u svim državama članicama.

Nezavisni nadzor ključni je element evropskog prava zaštite podataka. I prema pravu EU i pravu Saveta Evrope, postojanje nezavisnih nadzornih tela smatra se neophodnim za delotvornu zaštitu prava i sloboda pojedinaca u pogledu obrade njihovih ličnih podataka. Budući da je danas obrada podataka sveprisutna i sve složenija, pa je teško razumljiva prosečnoj osobi, ta su tela čuvari digitalnog doba. Postojanje nezavisnih nadzornih tela u EU smatra se jednim od osnovnih elemenata prava na zaštitu ličnih podataka i zaštićen je primarnim pravom Unije. Članom 8. stav 3. Povelje Evropske unije o osnovnim pravima i članom 16. stav 2. UFEU zaštita ličnih podataka prepoznaje se kao osnovno pravo i potvrđuje se da usklađenost s propisima o zaštiti podataka podleže kontroli nezavisnog tela.

Važnost nezavisnog nadzora za pravo zaštite podataka potvrđena je i sudskom praksom.

Primer: U predmetu *Schrems*[491] SPEU je razmatrao da li je prosleđivanje ličnih podataka u Sjedinjene Američke Države (SAD) u sklopu prvog Sporazuma o sigurnoj luci između EU i SAD u skladu sa zakonodavstvom EU o zaštiti podataka u kontekstu otkrića Edvarda Snoudena o masovnom nadzoru Nacionalne sigurnosne agencije (NSA) SAD. Prenos ličnih podataka u SAD zasnivao se na odluci Evropske komisije donesenoj 2000. godine, prema kojoj je dopušten prenos ličnih podataka iz organizacija u EU organizacijama u SAD, koje vrše vlastito potvrđivanje u sklopu sistema sigurne luke, na osnovu toga da se sistemom obezbeđuje odgovarajući nivo zaštite ličnih podataka. Kada je primilo

491 SPEU, C-362/14, *Maximillian Schrems protiv Data Protection Commissioner* [VV], 6. oktobra 2015.

zahtev za ispitivanje zakonitosti prenosa podataka nakon Snoudenovih otkrića, irsko nadzorno telo odbilo je zahtev, uz obrazloženje da Odluka Komisije o primerenosti režima zaštite podataka SAD, koji se odražava u načelima „sigurne luke" („Odluka o sigurnoj luci"), sprečava dalje ispitivanje tužbe.

Međutim, SPEU je smatrao da postojanje Odluke Komisije, koja omogućava prenos podataka u treće zemlje koje osiguravaju odgovarajuće nivoe zaštite, ne podrazumeva ukidanje niti smanjivanje ovlašćenja domaćih nadzornih tela. SPEU je istakao kako ovlašćenja tih tela u oblasti praćenja i obezbeđivanja usklađenosti s propisima EU o zaštiti podataka proizlaze iz primarnog prava EU, tačnije člana 8. stav 3. Povelje i člana 16. stav 2. UFEU. „Stoga je uspostavljanje nezavisnih nadzornih nacionalnih tela [...] osnovni deo poštovanja zaštite pojedinaca u vezi s obradom ličnih podataka."[492]

SPEU je zato odlučio da čak i kada je prenos ličnih podataka podvrgnut odluci Komisije o primerenosti, ako je prigovor podnesena domaćem nadzornom telu, to telo mora da ispita prigovor s dužnom pažnjom. Nadzorno telo može da odbije prigovor ako zaključi da je neutemeljen. U tom slučaju, SPEU je istakao da pravo na delotvoran pravni lek pred sudom podrazumeva da pojedinci moraju da imaju mogućnost pobijanja takve odluke pred domaćim sudovima, koji mogu da upute prethodno pitanje SPEU u vezi sa valjanošću odluke Komisije. Kada nadzorno telo smatra da je prigovor utemeljen, mora da ima moć da učestvuje u sudskom postupku i iznese predmet pred domaće sudove. Domaći sudovi mogu uputiti predmet SPEU-u jer je to jedino telo koje ima ovlašćenje za odlučivanje o valjanosti odluke o primerenosti Evropske komisije[493].

SPEU je zatim preispitao valjanost Odluke o sigurnoj luci kako bi utvrdio da li je sistem prenosa u skladu sa propisima EU-a o zaštiti podataka. Zaključio je da se članom 3. Odluke o sigurnoj luci ograničavaju ovlašćenja domaćih nadzornih tela (koja su im dodeljena Direktivom o zaštiti podataka) da preduzmu mere za sprečavanje prenosa podataka u slučaju neodgovarajućeg nivoa zaštite ličnih podataka u SAD. S obzirom na važnost nezavisnih nadzornih tela za osiguranje usklađenosti sa pravom zaštite podataka, SPEU je smatrao da na osnovu Direktive o zaštiti podataka i Povelje Komisija nije ovlašćena za ograničavanje ovlašćenja nezavisnim nadzornim telima na taj način. Ograničenje ovlašćenja nadzornih tela bilo je jedan od razloga zbog kojih je SPEU Odluku o sigurnoj luci proglasio nevažećom.

492 SPEU, C-362/14, *Maximillian Schrems protiv Data Protection Commissioner* [VV], 6. oktobra 2015, stav 41.

493 *Ibid*., st. od 53 do 66.

Evropskim pravom zato se zahteva nezavisan nadzor kao važan mehanizam za obezbeđivanje delotvorne zaštite podataka. Nezavisna nadzorna tela prva su tačka kontakta za ispitanike u slučajevima povreda podataka[494]. Unutar prava Unije i Saveta Evrope obavezno je uspostavljanje nadzornih tela. U oba pravna okvira opisuju se zadaci i ovlašćenja tih tela na sličan način kao i u OUZP-u. Stoga bi nadzorna tela, u načelu, trebalo da funkcionišu na isti način unutar prava EU i Saveta Evrope[495].

5.1. Nezavisnost

Pravom EU i **Saveta Evrope** propisuje se da svako nadzorno telo deluje potpuno nezavisno pri obavljanju svojih dužnosti i izvršavanju svojih ovlašćenja[496]. Nezavisnost nadzornog tela i njegovih članova, kao i osoblja, od neposrednih ili posrednih spoljnih uticaja ključno je za obezbeđivanje potpune objektivnosti pri donošenju odluka o pitanjima zaštite podataka. Osim što zakonodavstvo na kojem se zasniva osnivanje nadzornog tela mora sadržiti odredbe koje izričito garantuju nezavisnost, i sama organizaciona struktura tela mora biti dokaz njegove nezavisnosti. SPEU je 2010. godine prvi put razmatrao meru u kojoj nadzorna tela za zaštitu podataka moraju biti nezavisna[497]. Navedeni primeri ilustruju definiciju SPEU u značenju „potpune nezavisnosti".

Primer: U predmetu *Evropska komisija protiv Savezne Republike Nemačke*[498] Evropska komisija zatražila je od SPEU da utvrdi da je Nemačka netačno prenela zahtev „potpune nezavisnosti" nadzornih tela odgovornih za obezbeđenje zaštite podataka i na taj način nije ispunila svoje obaveze iz člana 28. stav 1. Direktive o zaštiti podataka. Prema mišljenju Komisije, Nemačka je prekršila zahtev nezavisnosti time što je pod nadzor države stavila tela odgovorna za nadzor obrade ličnih podataka u različitim saveznim državama (*Länder*) kako bi obezbedila usklađenost sa zakonodavstvom o zaštiti podataka.

SPEU je istakao da se reči „potpuno nezavisno" moraju tumačiti na osnovu stvarnog teksta te odredbe i na osnovu ciljeva i sistema zakonodavstva EU

494 Opšta uredba o zaštiti podataka, član 13. stav 2. tačka (d).

495 *Ibid*., član 51.; modernizovana Konvencija br. 108, član 15.

496 Opšta uredba o zaštiti podataka, član 52. stav 1.; modernizovana Konvencija br. 108, član 15. stav 5.

497 FRA (2010.), Temeljna prava: izazovi i postignuća u 2010., Godišnji izveštaj za 2010., str. 59; FRA (2010.), Zaštita podataka u Evropskoj uniji: uloga nacionalnih tela za zaštitu podataka, maj 2010.

498 SPEU, C-518/07, *Evropska komisija protiv Savezne Republike Nemačke* [VV], 9. marta 2010, stav 27.

o zaštiti podataka[499]. SPEU je naglasio da su nadzorna tela „čuvari" prava povezanih s obradom ličnih podataka. Stoga se smatra da je njihova uspostava u državama članicama „osnovni deo poštovanja zaštite pojedinaca u vezi s obradom ličnih podataka"[500]. SPEU je zaključio da „u izvršavanju svojih obaveza nadzorna tela moraju postupati objektivno i nepristrasno. Zbog toga moraju biti lišena svih spoljašnjih uticaja, uključujući neposredan ili posredan uticaj javnih tela"[501].

SPEU je takođe utvrdio da značenje „potpune nezavisnosti" treba tumačiti u svetlu nezavisnosti EDPS-a kako je definisana u Uredbi o zaštiti podataka u institucijama Evropske unije. U toj Uredbi konceptom nezavisnosti podrazumeva se da EDPS ne sme ni tražiti niti prihvatati uputstva drugih.

U skladu s tim, SPEU je smatrao da nemačka nadzorna tela nisu bila potpuno nezavisna u smislu zakonodavstva EU o zaštiti podataka jer su ih nadgledala javna tela.

Primer: U predmetu *Evropska komisija protiv Republike Austrije*[502] SPEU je naglasio slične probleme u vezi sa nezavisnošću određenih članova i osoblja austrijskog tela za zaštitu podataka (Komisija za zaštitu podataka, DSK/KZP). SPEU je zaključio da je Savezni kancelar prekršio zahtev nezavisnosti utvrđen u zakonodavstvu EU o zaštiti podataka jer je obezbedio radnu snagu nadzornog tela. SPEU je takođe smatrao da se zahtevom za informisanje Kancelara o njegovom radu u svakom trenutku poništava potpuna nezavisnost nadzornog tela.

Primer: U predmetu *Evropska komisija protiv Mađarske*[503] zabranjene su slične nacionalne prakse koje su uticale na nezavisnost radne snage. SPEU je istakao da „zahtev [...] da svako nadzorno telo izvršava funkcije koje su mu poverene potpuno nezavisno obavezuje državu članicu o kojoj se radi da poštuje trajanje mandata takvog nacionalnog tela do isteka roka koji je prvobitno predviđen". SPEU je takođe smatrao da je „okončavši prevremeno mandat nezavisnog nadzornog tela za zaštitu ličnih podataka, Mađarska povredila obaveze koje ima na osnovu Direktive 95/46 [...]".

499 *Ibid.*, st. 17 i 29.

500 *Ibid.*, stav 23.

501 *Ibid.*, stav 25.

502 SPEU, C-614/10, *Evropska komisija protiv Republike Austrije* [VV], 16. oktobra 2012, st. 59 i 63.

503 SPEU, C-288/12, *Evropska komisija protiv Mađarske* [VV], 8. aprila 2014. st. 50 i 67.

Pojam i kriterijumi „potpune nezavisnosti" sada su izričito utvrđeni u OUZP-u, koji sadrži načela uspostavljena presudama SPEU. U skladu sa Uredbom, potpuna nezavisnost pri obavljanju zadataka ili izvršavanju ovlašćenja podrazumeva sledeće[504]:

- članovi svakog nadzornog tela moraju biti slobodni od spoljašnjeg uticaja, bilo direktnog bilo indirektnog, i ne smeju da traže niti primaju uputstva ni od koga,
- članovi svakog nadzornog tela moraju da se suzdržavaju od svih radnji koje nisu u skladu sa njihovim dužnostima kako bi se sprečio sukob interesa,
- države članice moraju obezbediti da svako nadzorno telo ima ljudske, tehničke i finansijske resurse kao i infrastrukturu potrebnu za delotvorno obavljanje svojih zadataka,
- države članice moraju obezbediti da svako nadzorno telo bira vlastito osoblje,
- finansijska kontrola kojoj svako nadzorno telo podleže u skladu sa domaćim zakonodavstvom ne sme da utiče na njegovu nezavisnost. Nadzorna tela moraju imati zasebne, javne godišnje budžete koji im omogućavaju pravilan rad.

Nezavisnost nadzornih tela smatra se ključnim zahtevom i na osnovu prava Saveta Evrope. Modernizovanom Konvencijom br. 108 utvrđuje se da bi svako nadzorno telo „pri obavljanju svojih dužnosti i izvršavanju svojih ovlašćenja trebalo da deluje potpuno nezavisno i nepristrasno", bez traženja ili prihvatanja uputstava[505]. Na taj se način Konvencijom potvrđuje da ta tela ne mogu delotvorno štititi prava i slobode pojedinaca u vezi s obradom podataka ako ne mogu da vrše svoje funkcije potpuno nezavisno. U Izveštaju s objašnjenjima o modernizovanoj Konvenciji br. 108 utvrđuje se niz elemenata koji doprinose zaštiti te nezavisnosti. Ti elementi uključuju mogućnost da nadzorna tela zapošljavaju svoje osoblje i donose odluke bez spoljašnjeg uticaja, kao i faktore povezane s trajanjem njihovih funkcija i uslovima u kojima mogu prestati da vrše te funkcije[506].

504 Opšta uredba o zaštiti podataka, član 52.

505 Modernizovana Konvencija br. 108, član 15. stav 5.

506 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108.

5.2. Nadležnost i ovlašćenja

Prema pravu EU, u OUZP-u se navode nadležnosti i organizaciona struktura nadzornih tela, te se propisuje da ona moraju da budu nadležna i imaju ovlašćenja za izvršavanje zadataka utvrđenih u Uredbi.

Nadzorno telo je glavno telo u sklopu domaćegg zakonodavstva koje obezbeđuje usklađenost sa pravom zaštite EU. Osim praćenja, nadzorna tela imaju širok spektar zadataka i ovlašćenja koje uključuju proaktivne i preventivne aktivnosti nadzora. Kako bi izvršavala te zadatke, nadzorna tela moraju da imaju odgovarajuća istražna, korektivna i savetodavna ovlašćenja utvrđena u članovima 57. i 58. OUZP-a, kao što su[507]:

- savetovanje rukovaoca podacima i ispitanika o svim aspektima zaštite podataka,
- odobravanje standardnih ugovornih klauzula, obavezujućih korporativnih pravila ili administrativnih dogovora,
- istraživanje postupaka obrade i preduzimanje mera u skladu sa tim,
- zahtevanje svih informacija koje su važne za nadzor aktivnosti rukovaoca podacima,
- izdavanje upozorenja ili službenih opomena rukovaocima podacima i naređivanje rukovaocima podacima da ispitanike obaveste o povredama ličnih podataka,
- naređivanje ispravljanja, blokiranja, brisanja ili uništenja podataka,
- nametanje privremene ili konačne zabrane obrade ili izricanje upravne novčane kazne,
- upućivanje predmeta sudu.

Kako bi moglo da izvršava svoje funkcije, nadzorno telo mora da ima pristup svim ličnim podacima i informacijama nužnim za istragu, kao i pristup svim prostorijama u kojima rukovalac podacima čuva odgovarajuće informacije. Prema SPEU, ovlašćenja

507 Opšta uredba o zaštiti podataka, čl. 57. i 58. Vidi i Konvenciju br. 108, Dodatni protokol, član 1.

nadležnog tela moraju se široko tumačiti kako bi se obezbedila potpuna delotvornost zaštite podataka za ispitanike u EU.

Primer: U predmetu *Schrems* SPEU je razmatrao da li je prenos ličnih podataka u SAD u sklopu prvog Sporazuma o sigurnoj luci između EU i SAD u skladu sa pravom zaštite podataka EU u kontekstu otkrića Edvarda Snoudena. SPEU je zaključio da domaća nadzorna tela koja deluju u svojstvu nezavisnih rukovalaca podacima, koju vrše rukovaoci podacima, mogu sprečiti prenos ličnih podataka u treću zemlju uprkos odluci o primerenosti ako postoje utemeljeni dokazi da u toj trećoj zemlji više nije zagarantovana odgovarajuća zaštita[508].

Svako nadzorno telo nadležno je za izvršavanje istražnih ovlašćenja i ovlašćenja intervencije unutar svog državnog područja. Međutim, budući da su aktivnosti rukovaoca podacima i obrađivača podataka često prekogranične, pa obrada podataka utiče na ispitanike u više država članica, postavlja se pitanje o podeli nadležnosti na različita nadzorna tela. SPEU je imao priliku da razmotri to pitanje u predmetu *Weltimmo*.

Primer: U predmetu *Weltimmo*[509] SPEU je razmatrao nadležnost domaćih nadzornih tela u pitanjima koja se odnose na organizacije koje nemaju sedište unutar njegove sudske nadležnosti. Veltimo je bilo kompanija sa registrovanim sedištem u Slovačkoj, koja je upravljala internet stranicom za posredovanje nekretninama u Mađarskoj. Oglašivači su podneli tužbu mađarskom nadzornom telu za zaštitu podataka zbog kršenja mađarskog zakona o zaštiti podataka, a to je telo nametnulo novčanu kaznu kompaniji Veltimo. Kompanija je osporila novčanu kaznu pred domaćim sudovima, pa je predmet prosleđen SPEU kako bi utvrdio da li Direktiva EU o zaštiti podataka dopušta nadzornim telima određene države članice da primeni sopstvene domaće zakone o zaštiti podataka na kompaniju s registrovanim sedištem u drugoj državi članici.

SPEU je protumačio član 4. stav 1. tačka (a) Direktive o zaštiti podataka tako da se njime dopušta primena zakona o zaštiti podataka određene države članice, koja nije država članica u kojoj rukovalac podacima ima registrovano sedište,

508 SPEU, C-362/14, *Maximillian Schrems protiv Data Protection Commissioner* [VV], 6. oktobra 2015, st. od 26 do 36 i od 40 do 41.

509 SPEU, C-230/14, *Weltimmo s. r. o. protiv Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1. oktobra 2015.

„ako nadzorno telo putem stabilnih aranžmana na području te države članice obavlja, čak i najmanju, efektivnu i stvarnu delatnost u okviru koje se ta obrada sprovodi". SPEU je istakao da je, na osnovu informacija koje su mu iznesene, kompanija Veltimo obavljala stvarnu i efektivnu delatnost u Mađarskoj, jer je imala zastupnika u Mađarskoj koji je naveden u slovačkom registru kompanija pod adresom koja se nalazi u Mađarskoj, otvorio je bankovni račun u Mađarskoj i raspolagao poštanskim pretincem, te takođe obavljao aktivnosti u Mađarskoj putem internet stranica sastavljenih na mađarskom jeziku. Te informacije su ukazivale na postojanje sedišta, čime bi aktivnosti kompanije Veltimo podlegale mađarskom zakonu o zaštiti podataka i nadležnosti mađarskog nadzornog tela. Međutim, SPEU je domaćem sudu prepustio proveru informacija i odluku o tome da li Veltimo ima sedište u Mađarskoj.

Ako bi sud, koji je uputio prethodno pitanje SPEU, utvrdio da Veltimo ima sedište u Mađarskoj, mađarsko nadzorno telo bi imalo ovlašćenje da izrekne novčanu kaznu. Sa druge strane, ako bi domaći sud doneo suprotnu odluku, odnosno da Veltimo nema sedište u Mađarskoj, merodavni zakon bi bio zakon države članice (ili država članica) u kojoj je ta kompanija registrovana. Budući da se u tom slučaju ovlašćenja nadzornih tela moraju izvršiti u skladu sa teritorijalnim suverenitetom drugih država članica, mađarsko telo ne bi moglo da izriče kazne. Budući da je Direktiva o zaštiti podataka sadržala odredbu o učešću nadzornih tela, mađarsko telo je moglo da zatraži od istovetnog slovačkog tela da ispita slučaj, utvrdi da je došlo do kršenja slovačkog zakona i izrekne kazne propisane slovačkim zakonodavstvom.

S donošenjem OUZP-a uspostavljeni su detaljni propisi o nadležnosti nadzornih tela u prekograničnim slučajevima. Uredbom je uspostavljen „jedinstveni mehanizam" tako da su utvrđene odredbe o saradnji različitih nadzornih tela. Radi efikasne saradnje u prekograničnim slučajevima, OUZP-om se propisuje da vodeće nadzorno telo bude uspostavljeno kao nadzorno telo glavnog ili jedinog sedišta rukovaoca podacima ili obrađivača podataka[510]. Vodeće nadzorno telo nadležno je za prekogranične predmete, jedini je sagovornik rukovaoca ili obrađivača podataka i koordinira saradnju s drugim nadzornim telima kako bi se postigao konsenzus. Saradnja uključuje razmenu informacija, uzajamnu pomoć u praćenju i vođenju istraga, kao i donošenje obavezujućih odluka[511].

510 Opšta uredba o zaštiti podataka, član 56. stav 1.

511 *Ibid.*, član 60.

U okviru prava Saveta Evrope, nadležnosti i ovlašćenja nadzornih tela utvrđene su članom 15. modernizovane Konvencije br. 108. Ta ovlašćenja odgovaraju ovlašćenjima koja su nadzornim telima dodeljena pravom Unije, uključujući ovlašćenja za istraživanje i intervenciju, ovlašćenja za donošenje odluka i izricanje upravnih kazni za kršenje odredbi Konvencije, kao i ovlašćenja za učestvovanje u sudskim postupcima. Nezavisna nadzorna tela takođe su nadležna za obradu zahteva i prigovora koje podnesu ispitanici, za podizanje svesti javnosti o zakonodavstvu o zaštiti podataka i za savetovanje domaćih donosilaca odluka u vezi sa svim zakonodavnim ili upravnim merama kojima se reguliše obrada ličnih podataka.

5.3. Saradnja

OUZP-om se uspostavlja opšti okvir saradnje nadzornih tela i utvrđuju konkretna pravila saradnje nadzornih tela u prekograničnim aktivnostima obrade podataka.

U skladu sa OUZP-om, nadzorna tela pružaju jedno drugom uzajamnu pomoć i dele relevantne informacije radi doslednog sprovođenja i primene Uredbe[512]. To uključuje da nadzorno telo na zahtev sprovodi savetovanja, inspekcije i istrage. Nadzorna tela mogu da sprovode zajedničke operacije, uključujući zajedničke istrage i zajedničke mere sprovođenja u kojima učestvuje osoblje svih nadzornih tela[513].

U EU rukovaoci podacima i obrađivači podataka sve više deluju na transnacionalnom nivou. To zahteva blisku saradnju nadležnih nadzornih tela u državama članicama kako bi se obezbedilo da obrada ličnih podataka bude u skladu sa zahtevima OUZP-a. Prema „jedinstvenom mehanizmu" iz Uredbe, ako rukovalac podacima ili obrađivač podataka ima sedišta u nekoliko država članica ili ako ima jedno sedište, ali postupci obrade značajno utiču na ispitanike u više od jedne države članice, nadzorno telo glavnog (ili jedinog) sedišta vodeće je nadzorno telo za prekogranične aktivnosti rukovaoca podacima ili obrađivača podataka. Vodeća nadzorna tela su ovlašćena da sprovedu mere protiv rukovaoca podacima ili obrađivača podataka. Cilj jedinstvenog mehanizma je da se poboljšaju usklađenost i ujednačeno sprovođenje zakonodavstva EU o zaštiti podataka u različitim državama članicama. On je koristan i za preduzeća jer, zahvaljujući njemu, ona treba da sarađuju samo sa vodećim nadzornim telom umesto s nekoliko različitih nadzornih tela. Time se povećava pravna sigurnost za preduzeća, a u praksi bi to takođe trebalo da znači da se odluke brže

512 *Ibid.*, član 61. st. od 1 do 3 i član 62. stav 1.

513 *Ibid.*, član 62. stav 1.

donose i da preduzeća ne moraju da se nose s protivrečnim zahtevima koje nameću različita nadzorna tela.

Određivanje vodećeg nadzornog tela podrazumeva utvrđivanje lokacije glavnog sedišta preduzeća u EU. Pojam „glavnog sedišta" definisan je u OUZP-u. Usto, Radna grupa iz člana 29. objavila je smernice za utvrđivanje vodećeg nadzornog tela ili obrađivača podataka koje uključuju kriterijume za određivanje glavnog sedišta[514].

Kako bi se obezbedio visok nivo zaštite podataka u celoj EU, vodeće nadzorno telo ne deuje samostalno. Ono mora da sarađuje s drugim nadležnim nadzornim telima na donošenju odluka o obradi ličnih podataka koju obavljaju rukovaoci podacima i obrađivači podataka kako bi se postigao konsenzus i obezbedila doslednost. Saradnja relevantnih nadzornih tela uključuje razmenu informacija, uzajamnu pomoć, sprovođenje zajedničkih istraga i aktivnosti praćenja[515]. Prilikom pružanja uzajamne pomoći, nadzorna tela moraju pravilno da postupaju sa zahtevima za informacije koje upute druga nadzorna tela i da sprovode mere nadzora, kao što su prethodno odobravanje i savetovanje s rukovaocem podacima u vezi s njegovim aktivnostima obrade, inspekcije i istrage. Uzajamna pomoć nadzornim telima u drugim državama članicama mora se pružiti na zahtev bez nepotrebnog odlaganja i najkasnije u roku od mesec dana posle prijema zahteva[516].

Kada rukovalac podacima ima sedišta u nekoliko država članica, nadzorna tela mogu da sprovode zajedničke operacije, uključujući istrage i mere sprovođenja u kojima učestvuju članovi osoblja nadzornih tela drugih država članica[517].

Saradnja različitih nadzornih tela važan je zahtev i prema pravu Saveta Evrope. Modernizovanom Konvencijom br. 108 utvrđuje se da nadzorna tela moraju međusobno da sarađuju u meri potrebnoj za izvršavanje svojih zadataka[518]. To treba činiti, na primer, razmenom svih relevantnih i korisnih informacija, koordinacijom istraga i sprovođenjem zajedničkih aktivnosti[519].

514 Radna grupa iz člana 29. (2016.), *Smernice za identifikaciju voditelja obrade ili vodećeg nadzornog tela izvršitelja obrade*, WP 244, Bruxelles, 13. decembra 2016., revidirane 5. aprila 2017.

515 Opšta uredba o zaštiti podataka, član 60 st. od 1 do 3.

516 *Ibid*., član 61. st. 1 i 2.

517 *Ibid*., član 62. stav 1.

518 Modernizovana Konvencija br. 108, čl. 16. i 17.

519 *Ibid*., član 17.

5.4. Evropski odbor za zaštitu podataka

Važnost nezavisnih nadzornih tela i glavne nadležnosti koje imaju prema evropskom zakonodavstvu o zaštiti podataka opisane su u prethodnom delu ovog poglavlja. Evropski odbor za zaštitu podataka (EOZP) drugi je važan učesnik u obezbeđenju efikasne i dosledne primene propisa o zaštiti podataka na nivou EU.

OUZP-om je Odbor osnovan kao telo EU koje ima pravnu ličnost[520]. On je naslednik Radne grupe iz člana 29.[521], koja je osnovana Direktivom o zaštiti podataka kako bi savetovala Komisiju o svim merama EU koje utiču na prava pojedinaca u pogledu obrade ličnih podataka i privatnosti, unapređivala ujednačenu primenu Direktive i Komisiji pružala stručna mišljenja o pitanjima u vezi sa zaštitom podataka. Radna grupa iz člana 29. sastojala se od predstavnika nadzornih tela iz država članica EU, kao i predstavnika Komisije i EDPS-a.

Slično kao i Radna grupa, EOZP čine rukovodioci nadzornih tela iz svake države članice i EDPS-a ili njihovi predstavnici[522]. EDPS ima jednaka prava glasa, uz izuzetak predmeta koji su povezani s rešavanjem sporova, u kojima može glasati samo o odlukama koje se odnose na načela i propise primenjive na institucije EU koji su u suštini usklađeni sa onima iz OUZP-a. Komisija ima pravo učešća u aktivnostima i sastancima Odbora, ali nema pravo glasa[523]. Odbor bira predsednika (koji je ujedno predstavnik Odbora) i dva zamenika predsednika iz redova svojih članova natpolovičnom većinom na period od pet godina. EOZP takođe ima sekretarijat koji obezbeđuje Evropski nadzornik za zaštitu podataka radi analitičke, administrativne i logističke pomoći Odboru[524].

Zadaci EOZP-a detaljno su navedeni u članovima 64., 65. i 70. Opšte uredbe o zaštiti podataka, a uključuju sveobuhvatne dužnosti koje se mogu podeliti u tri glavne aktivnosti:

- **Doslednost:** EOZP može da donosi pravno obavezujuće odluke u tri slučaja: ako nadzorno telo podnese relevantan i obrazložen prigovor kad je reč o jedinstvenim

520 Opšta uredba o zaštiti podataka, član 68.

521 U skladu sa Direktivom 95/46/EZ, Radna grupa iz člana 29. trebalo je da savetuje Komisiju o svim merama EU koje utiču na prava pojedinaca u pogledu obrade ličnih podataka i privatnosti, unapređuje ujednačenu primenu Direktive i pruža stručna mišljenja Komisiji o pitanjima povezanima sa zaštitom podataka. Radna grupa iz člana 29. sastojala se od predstavnika nadzornih tela iz država članica EU, Komisije i EDPS-a.

522 Opšta uredba o zaštiti podataka, član 68. stav 3.

523 *Ibid*., član 68. st. 4 i 5.

524 *Ibid*., članovi 73. i 75.

kontakt tačkama, ako postoje oprečna mišljenja o tome koje je nadzorno telo „vodeće" i, konačno, ako nadležno nadzorno telo ne zatraži ili ne uzme u obzir mišljenje EOZP-a[525]. Glavna odgovornost EOZP-a je da obezbedi dosledno sprovođenje Uredbe na nivou EU, tako da on igra ključnu ulogu u mehanizmu doslednosti, koji je opisan u delu 5.5.

- **Savetovanje:** zadaci EOZP-a uključuju savetovanje Komisije o svim pitanjima u pogledu zaštite ličnih podataka u Uniji, poput izmena OUZP-a, revizija zakonodavstva EU koje se odnosi na obradu podataka i koje može da bude u sukobu s propisima EU o zaštiti podataka, ili izdavanja odluka o primerenosti Evropske komisije koje omogućavaju prenos ličnih podataka trećim zemljama ili međunarodnim organizacijama.

- **Smernice:** Odbor, takođe, izdaje smernice, preporuke i primere najbolje prakse kako bi podstakao dosledno izvršenje Uredbe i unapređuje saradnju i razmenu znanja među nadzornim telima. Usto mora podsticati udruženja rukovalaca podacima ili obrađivača podataka da izrađuju kodekse ponašanja i uspostave mehanizme sertifikovanja i pečata za zaštitu podataka.

Odluke EOZP-a mogu da se ospore pred SPEU.

5.5. Mehanizam doslednosti iz Opšte uredbe o zaštiti podataka

OUZP-om se uspostavlja mehanizam doslednosti kojim se obezbeđuje da se Uredba dosledno sprovodi u svim državama članicama putem međusobne saradnje nadzornih tela i, po potrebi, njihove saradnje sa Komisijom. Mehanizam doslednosti primenjuje se u dva slučaja. Prvi slučaj se odnosi na mišljenja EOZP-a u slučajevima u kojima nadzorno telo namerava da donese mere poput liste postupaka obrade koji zahtevaju procenu efekta zaštite podataka (DPIA) ili određivanja standardnih ugovornih klauzula. Drugi slučaj se odnosi na obavezujuće odluke EOZP-a za nadzorna tela u slučajevima jedinstvene kontakt tačke i kada nadzorno telo ne uzima u obzir ili ne zatraži mišljenje EOZP-a.

525 *Ibid.*, član 65.

6

Prava ispitanika i njihovo sprovođenje

EU	Obuhvaćena pitanja	Savet Evrope
Pravo na informacije		
Opšta uredba o zaštiti podataka, član 12. SPEU, C-473/12, *Institut professionnel des agents immobiliers (IPI) protiv Engleberta*, 2013. SPEU, C-201/14, *Smaranda Bara i dr. protiv Casa Națională de Asigurări de Sănătate i dr.*, 2015.	Transparentnost informacija	Modernizovana Konvencija br. 108, član 8.
Opšta uredba o zaštiti podataka, član 13. stavovi 1. i 2. i član 14. stavovi 1. i 2.	Sadržaj informacija	Modernizovana Konvencija br. 108, član 8. stav 1.
Opšta uredba o zaštiti podataka, član 13. stav 1. i član 14. stav 3.	Vreme pružanja informacija	Modernizovana Konvencija br. 108, član 9. stav 1. tačka (b)
Opšta uredba o zaštiti podataka, član 12. stavovi 1., 5. i 7.	Način pružanja informacija	Modernizovana Konvencija br. 108, član 9. stav 1. tačka (b)
Opšta uredba o zaštiti podataka, član 13. stav 2. tačka (d), član 14. stav 2. tačka (e) i članovi 77., 78. i 79.	Pravo na podnošenje tužbe	Modernizovana Konvencija br. 108, član 9. stav 1. tačka (f)
Pravo na pristup		
Opšta uredba o zaštiti podataka, član 15. stav 1. SPEU, C-553/07, *College van burgemeester en wethouders van Rotterdam protiv M. E. E. Rijkeboer*, 2009.	Pravo na pristup sopstvenim podacima	Modernizovana Konvencija br. 108, član 9. stav 1. tačka (b) ESLJP, *Leander protiv Švedske*, br. 9248/81, 1987.

EU	Obuhvaćena pitanja	Savet Evrope
SPEU, spojeni predmeti C-141/12 i C-372/12, *Y. S. protiv Minister voor Immigratie, Integratie en Asiel i Minister voor Immigratie, Integratie en Asiel protiv M. i S.*, 2014. SPEU, C-434/16, *Peter Nowak protiv Data Protection Commissioner*, 2017.		
Pravo na ispravku		
Opšta uredba o zaštiti podataka, član 16.	Ispravka netačnih ličnih podataka	Modernizovana Konvencija br. 108, član 9. stav 1. tačka (e) ESLJP, *Cemalettin Canli protiv Turske*, br. 22427/04, 2008. ESLJP, *Ciubotaru protiv Moldavije*, br. 27138/04, 2010.
Pravo na brisanje		
Opšta uredba o zaštiti podataka, član 17. stav 1.	Brisanje ličnih podataka	Modernizovana Konvencija br. 108, član 9. stav 1. tačka (e) ESLJP, *Segerstedt-Wiberg i drugi protiv Švedske*, br. 62332/00, 2006.
SPEU, C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González* [VV], 2014. SPEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce protiv Salvatorea Mannija*, 2017.	Pravo na zaborav	
Pravo na ograničenje obrade		
Opšta uredba o zaštiti podataka, član 18. stav 1.	Pravo na ograničenje upotrebe ličnih podataka	
Opšta uredba o zaštiti podataka, član 19.	Obaveza obaveštavanja	
Pravo na prenosivost podataka		
Opšta uredba o zaštiti podataka, član 20.	Pravo na prenosivost podataka	

EU	Obuhvaćena pitanja	Savet Evrope
Pravo na prigovor		
Opšta uredba o zaštiti podataka, član 21. stav 1. SPEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce protiv Salvatorea Mannija*, 2017.	Pravo na prigovor zbog posebne situacije ispitanika	Preporuka o izradi profila, član 5.3. Modernizovana Konvencija br. 108, član 9. stav 1. tačka (d)
Opšta uredba o zaštiti podataka, član 21. stav 2.	Pravo na prigovor na upotrebu podataka u marketinške svrhe	Preporuka o neposrednom marketingu, član 4.1.
Opšta uredba o zaštiti podataka, član 21. stav 5.	Pravo na prigovor automatizovanim putem	
Prava povezana s automatizovanim donošenjem odluka i izradom profila		
Opšta uredba o zaštiti podataka, član 22.	Prava povezana s automatizovanim donošenjem odluka i izradom profila	Modernizovana Konvencija br. 108, član 9. stav 1. tačka (a)
Opšta uredba o zaštiti podataka, član 21.	Pravo na prigovor na automatizovano donošenje odluka	
Opšta uredba o zaštiti podataka, član 13. stav 2. tačka (f)	Prava na smisleno pojašnjenje	Modernizovana Konvencija br. 108, član 9. stav 1. tačka (c)
Pravni lekovi, odgovornost, sankcije i naknada		
Povelja, član 47. SPEU, C-362/14, *Maximillian Schrems protiv Data Protection Commissioner* [VV], 2015. Opšta uredba o zaštiti podataka, članovi od 77. do 84.	Za kršenja domaćeg zakonodavstva o zaštiti podataka	Evropska konvencija o ljudskim pravima, član 13. (samo za države članice Saveta Evrope) Modernizovana Konvencija br. 108, član 9. stav 1. tačka (f) i članovi 12., 15. i od 16. do 21. ESLJP, *K. U. protiv Finske*, br. 2872/02, 2008. ESLJP, *Biriuk protiv Litvanije*, br. 23373/03, 2008.
Uredba o zaštiti podataka u institucijama Evropske unije, članovi 34. i 49. SPEU, C-28/08 P, *Evropska komisija protiv The Bavarian Lager Co. Ltd* [VV], 2010.	Za kršenja prava Evropske unije koju učine institucije i tela Evropske unije	

Efikasnost pravnih propisa uopštenono, a posebno prava ispitanika, u velikoj meri zavisi od postojanja odgovarajućih mehanizama za njihovo sprovođenje. U digitalnom dobu obrada podataka postala je sveprisutna i prosečna osoba je sve teže razume. Kako bi se umanjila neravnoteža moći između ispitanika i rukovaoca podacima, pojedinci imaju određena prava koja im omogućavaju ostvarenje veće kontrole nad obradom njihovih ličnih podataka. Pravo na pristup sopstvenim podacima i pravo na njihovu ispravku zagarantovane su članom 8. stav 2. Povelje EU o osnovnim pravima, dokumenta koji čini primarno pravo Unije i osnov je pravnog poretka EU. Sekundarnim pravom Unije, a naročito Opštom uredbom o zaštiti podataka, uspostavlja se usklađen pravni okvir koji ispitanicima stavlja na raspolaganje prava koja se odnose na rukovaoce podacima. Uz pravo na pristup i ispravku, OUZP-om se utvrđuje niz drugih prava, kao što su pravo na brisanje („pravo na zaborav"), pravo na prigovor ili na ograničenje obrade podataka, kao i prava povezanih s automatizovanim donošenjem odluka i izradom profila. Slične zaštitne mere putem kojih ispitanici mogu da preuzmu kontrolu nad svojim podacima utvrđene su i u modernizovanoj Konvenciji br. 108. U članu 9. navedena su prava koja pojedinci treba da imaju na raspolaganju u vezi s obradom njihovih ličnih podataka. Ugovorne strane moraju biti sigurne da su ta prava dostupna svakom ispitaniku u njihovoj oblasti nadležnosti i da su ona propraćena delotvornim pravnim i praktičnim merama kako bi ispitanici mogli da ih ostvare.

Uz davanje prava pojedincima, podjednako je važno uspostaviti mehanizme koji ispitanicima omogućavaju da ulože prigovor na kršenje svojih prava, pozovu rukovaoce podacima na odgovornost i zatraže naknadu štete. Pravo na delotvoran pravni lek, zagarantovan EKLJP-om i Poveljom, podrazumeva da su pravni lekovi dostupni svakom licu.

6.1. Prava ispitanika

Ključne tačke

- Svaki ispitanik ima pravo na informacije o svakoj obradi koju rukovalac podacima vrši na njegovim ličnim podacima, uz određena ograničena izuzeća.
- Ispitanici imaju pravo na:
  - pristup sopstvenim podacima i dobijanje određenih informacija o njihovoj obradi,
  - ispravku svojih podataka, ako su netačni, koju vrši rukovalac podacima koji ih obrađuje,

  - brisanje svojih podataka koje po potrebi vrši rukovalac podacima ako podatke obrađuje nezakonito,
  - privremeno ograničenje obrade,
  - prenos svojih podataka drugom rukovaocu podacima u određenim uslovima.
- Osim toga, ispitanici imaju pravo na prigovor na obradu s obzirom na:
  - osnovu koja se odnosi na njihovu posebnu situaciju,
  - upotrebu njihovih podataka u svrhu ciljanog marketinga.
- Ispitanici imaju pravo na to da se o njima ne donose odluke koje se temelje isključivo na automatizovanoj obradi, uključujući izradu profila, a koje imaju pravni efekat ili koje značajno utiču na njih. Ispitanici takođe imaju pravo na:
  - ljudsku intervenciju rukovaoca podacima,
  - izražavanje sopstvenog stava kao i osporavanje odluke koja se temelji na automatizovanoj obradi.

6.1.1. Pravo na informacije

Prema **pravu Saveta Evrope** i **pravu EU**, rukovaoci podacima dužni su da obaveste ispitanika o svrsi obrade u trenutku prikupljanja ličnih podataka. Ta obaveza ne zavisi od zahteva ispitanika, nego rukovalac podacima mora proaktivno ispunjavati tu obavezu, nezavisno od toga da li ispitanik pokazuje interesovanje za informacije ili ne.

Prema pravu Saveta Evrope, u skladu sa članom 8. modernizovane Konvencije br. 108, ugovorne strane moraju obezbediti da rukovaoci podacima obaveste ispitanike o svom identitetu i uobičajenom boravištu, pravnoj osnovi i svrsi obrade, kategorijama ličnih podataka koji se obrađuju, primaocima njihovih ličnih podataka (ako postoje), kao i o tome kako mogu ostvariti svoja prava na osnovu člana 9., koja uključuju pravo na pristup, ispravku i pravni lek. Ispitanicima treba saopštiti i sve druge dodatne informacije koje se smatraju nužnima za pravičnu i transparentnu obradu ličnih podataka. U Izveštaju s objašnjenjima o modernizovanoj Konvenciji br. 108 objašnjava se da informacije koje se daju ispitanicima „treba da budu jednostavno dostupne, čitljive, razumljive i prilagođene relevantnim ispitanicima”[526].

526 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 68.

U sklopu prava Unije, načelo transparentnosti podrazumeva da svaka obrada ličnih podataka generalno treba da bude transparentna za pojedince. Pojedinci imaju pravo da znaju kako se i koji lični podaci prikupljaju, upotrebljavaju ili drugačije obrađuju, kao i koji su rizici, zaštitne mere i njihova prava u vezi s obradom[527]. Članom 12. OUZP-a utvrđuje se široka sveobuhvatna obaveza za rukovaoce podacima prema kojoj moraju davati transparentne informacije i/ili saopštiti ispitanicima kako mogu da ostvare svoja prava[528]. Informacije moraju biti sažete, transparentne, razumljive i lako dostupne, kao i date na jasnom i jednostavnom jeziku. Informacije se moraju dati u pisanom obliku, što uključuje i davanje elektronskim putem ako je prikladno, a na zahtev ispitanika mogu se dati i usmenim putem, pod uslovom da je bez sumnje utvrđen njegov identitet. Informacije se daju bez prekomernog odlaganja ili naknade[529].

Članovi 13. i 14. OUZP-a odnose se na pravo ispitanika na informacije u slučajevima u kojima su lični podaci prikupljeni neposredno od njih, odnosno slučajevima u kojima nisu dobijeni od njih.

Opseg prava na informacije i njegova ograničenja na osnovu prava Unije pojašnjeni su u sudskoj praksi SPEU.

Primer: U predmetu *Institut professionnel des agents immobiliers (IPI) protiv Engleberta*[530] od SPEU se tražilo da tumači član 13. stav 1. Direktive 95/46/EZ. Tim članom je državama članicama pružena mogućnost izbora o donošenju zakonskih mera za ograničavanje oblasti primene prava ispitanika na informacije kada je to potrebno radi, između ostalog, zaštite prava i sloboda drugih i sprečavanja i istrage krivičnih dela ili kršenja etike zakonom uređenih delatnosti. IPI je strukovna organizacija agenata za nekretnine u Belgiji koja je odgovorna za obezbeđenje usklađenosti s odgovarajućim praksama delatnosti prodaje nekretnina. Ona je od domaćeg suda zatražila da presudi da su optuženi prekršili pravila delatnosti i da im naredi da obustave aktivnosti prodaje nekretnina. Postupak je pokrenut na osnovu dokaza koje su prikupili privatni istražitelji koje je IPI zaposlio.

527 Opšta uredba o zaštiti podataka, uvodna izjava 39.

528 *Ibid*., članovi 13. i 14; modernizovana Konvencija br. 108, član 8. stav 1. tačka (b).

529 Opšta uredba o zaštiti podataka, član 12. stav 5; modernizovana Konvencija br. 108, član 9. stav 1. tačka (b).

530 SPEU, C-473/12, *Institut professionnel des agents immobiliers (IPI) protiv Geoffreyja Engleberta i dr.*, 7. novembra 2013.

Domaći sud je imao sumnji u vezi sa vrednošću dokaza koje su dostavili istražitelji s obzirom na mogućnost da su prikupljeni bez poštovanja propisa o zaštiti podataka iz belgijskog zakonodavstva, a naročito obaveze da ispitanici budu obavešteni o obradi njihovih ličnih podataka pre prikupljanja takvih informacija. SPEU je istakao da je u članu 1. stav 1 utvrđeno da države članice „mogu", ali ne moraju da propišu izuzetke u svojim domaćim zakonodavstvima za obavezu obaveštavanja ispitanika o obradi njihovih podataka. Budući da član 13. stav 1. uključuje sprečavanje, istragu, otkrivanje i gonjenje krivičnih dela ili povredu etike kao osnove po kojima države članice mogu ograničiti prava pojedinaca, aktivnost tela poput IPI-ja i privatnih istražitelja koji deluju u njegovo ime može se zasnivati na toj odredbi. Međutim, ako država članica nije propisala takav izuzetak, ispitanici se moraju obavestiti.

Primer: U predmetu *Smaranda Bara i dr. protiv Casa Naţională de Asigurări de Sănătate i dr.*[531] SPEU je pojasnio da li se pravom EU sprečava prenos ličnih podataka jednog domaćeg tela javne uprave drugom telu javne uprave radi dalje obrade bez obaveštavanja ispitanika o prenosu i o obradi. U tom predmetu Državna agencija za upravljanje nije obavestila tužioce da je prenela njihove podatke Državnom fondu za socijalnu zaštitu pre samog prenosa.

SPEU je smatrao da je zahtev iz prava Unije za obaveštavanje ispitanika o obradi njihovih ličnih podataka „utoliko važniji što je reč o nužnoj pretpostavci za to da te osobe koriste svoje pravo na pristup i ispravljanje obrađenih podataka [...] i svoje pravo prigovora obradi spomenutih podataka". Prema načelu pravične obrade zahteva se obaveštavanje ispitanika o prenosu njihovih podataka drugom javnom telu radi dalje obrade. U skladu sa članom 13. stav 1. Direktive 95/46/EZ, države članice mogu ograničiti pravo na informacije ako se to smatra nužnim za zaštitu važnog ekonomskog interesa države, uključujući poreska pitanja. Međutim, takva ograničenja moraju da se sprovedu zakonskim merama. Budući da ni definicija podataka koji se prenose ni detaljni načini prenosa nisu utvrđeni zakonskom merom, nego isključivo protokolom između dvaju javnih tela, uslovi za odstupanje na osnovu prava Unije nisu ispunjeni. Trebalo je da tužioci budu unapred obavešteni o prenosu njihovih podataka Državnom fondu za socijalnu zaštitu, kao i o naknadnoj obradi podataka u tom telu.

531 SPEU, C-201/14, *Smaranda Bara i dr. protiv Casa Naţională de Asigurări de Sănătate i dr.*, 1. oktobra 2015.

Sadržaj informacija

U skladu sa članom 8. stav 1. modernizovane Konvencije br. 108, rukovalac podacima je dužan da da ispitaniku sve informacije kojima se obezbeđuje pravična i transparentna obrada ličnih podataka, uključujući sledeće:

- identitet i uobičajeno boravište ili sedište rukovaoca podacima,
- pravnu osnovu i predviđene svrhe obrade,
- kategorije obrađenih ličnih podataka,
- primaoce ili kategorije primalaca ličnih podataka, ako ih ima,
- načine na koje ispitanici mogu da ostvaruju svoja prava.

U skladu sa OUZP-om, ako su lični podaci prikupljeni od ispitanika, rukovalac podacima je dužan da u trenutku prikupljanja ličnih podataka da ispitaniku sledeće informacije[532]:

- identitet i kontakt podatke rukovaoca podacima i, ako je primenjivo, službenika za zaštitu podataka rukovaoca podacima,
- svrhu obrade i pravnu osnovu za obradu, tj. ugovornu ili zakonsku obavezu,
- legitimni interes rukovaoca podacima ako on čini osnovu za obradu,
- krajnje primaoce ili kategorije primalaca ličnih podataka,
- da li će se lični podaci preneti trećoj zemlji ili međunarodnoj organizaciji i da li se izbor zasniva na odluci o primerenosti ili odgovarajućim zaštitnim merama,
- period u kojem će lični podaci biti čuvani ili, ako nije moguće odrediti period, kriterijume prema kojima se utvrdio period čuvanja podataka,
- prava ispitanika u vezi s obradom, poput prava na pristup ličnim podacima, prava na ispravku, brisanje ili ograničavanje obrade podataka ili prava na prigovor na obradu,

532 Opšta uredba o zaštiti podataka, član 13. stav 1.

- da li je davanje ličnih podataka zakonska ili ugovorna obaveza, da li ispitanik ima obavezu davanja ličnih podataka i koje su moguće posledice ako se takvi podaci ne daju,
- postojanje automatizovanog donošenja odluka, uključujući izradu profila,
- pravo na podnošenje tužbe nadzornom telu,
- postojanje prava na povlačenje pristanka.

U slučajevima automatizovanog donošenja odluka, uključujući izradu profila, ispitanici moraju da dobiju smislene informacije o logici izrade profila, njenoj važnosti i predviđenim posledicama takve obrade.

U slučajevima u kojima lični podaci nisu dobijeni neposredno od ispitanika, rukovalac podacima mora da obavesti pojedinca o poreklu ličnih podataka. U svakom slučaju rukovalac podacima mora, između ostalog, da obavesti ispitanike o postojanju automatizovanog donošenja odluka, uključujući izradu profila[533]. Konačno, ako rukovalac podacima namerava da obrađuje lične podatke u svrhu koja je različita od one koja je izvorno navedena ispitaniku, prema načelima ograničenja svrhe i transparentnosti od rukovaoca podacima se zahteva da ispitaniku da informacije o toj novoj svrsi. Rukovaoci podacima moraju da daju informacije pre bilo kakve dalje obrade. Drugim rečima, u slučajevima u kojima je ispitanik dao pristanak za obradu ličnih podataka rukovalac podacima mora da dobije novi pristanak ispitanika ako se promeni svrha obrade ili se dodaju nove svrhe.

Vreme davanja informacija

U OUZP-u se razlikuju dve situacije i dva trenutka u kojima rukovalac podacima mora da dâ informacije ispitaniku.

- Ako su lični podaci prikupljeni neposredno od ispitanika, rukovalac podacima u trenutku prikupljanja podataka toj osobi mora da dâ sve relevantne informacije i prava koja ima na osnovu OUZP-a[534].
  Ako rukovalac podacima namerava da dodatno obrađuje lične podatke u drugu svrhu, pre te dodatne obrade daje sve relevantne informacije o tome.

533 Opšta uredba o zaštiti podataka, član 13. stav 2. i član 14. stav 2. tačka (f).

534 *Ibid*., član 13. st. 1. i 2., uvod u kojem se tekst Uredbe odnosi na obavezne informacije koje se moraju primeniti „u trenutku prikupljanja ličnih podataka".

- Ako lični podaci nisu dobijeni od ispitanika, rukovalac podacima dužan je da ispitaniku da informacije o obradi „unutar razumnog roka nakon dobijanja ličnih podataka, a najkasnije u roku od jednog meseca" ili pre otkrivanja podataka trećoj strani[535].

U Izveštaju s objašnjenjima o modernizovanoj Konvenciji br. 108 utvrđuje se da, ako obaveštavanje ispitanika nije moguće u trenutku započinjanja obrade, ono se može izvršiti u kasnijoj fazi, na primer, kada rukovalac podacima zbog bilo kojeg razloga stupi u kontakt s ispitanikom[536].

Različiti načini pružanja informacija

Prema pravu Saveta Evrope i EU, informacije koje je rukovalac podacima dužan da dâ ispitanicima moraju biti sažete, transparentne, razumljive i lako dostupne. Moraju se dati u pisanom obliku ili drugim sredstvima, uključujući one koje se daju elektronskim putem, uz upotrebu jasnog, jednostavnog i lako razumljivog jezika. Prilikom pružanja informacija rukovalac podacima može upotrebiti standardizovane ikone kako bi informacije bile dostupne na lako vidljiv i razumljiv način[537]. Na primer, ikona koja izgleda kao katanac može se upotrebiti kao oznaka bezbednog prikupljanja i/ili šifrovanja podataka. Ispitanici mogu zatražiti da im se informacije daju usmeno. Informacije moraju da se daju bez naknade, osim ako su zahtevi ispitanika očigledno neutemeljeni ili preterani (npr. zbog njihovog učestalog ponavljanja)[538]. Jednostavan pristup datim informacijama neophodan je za ostvarivanje prava ispitanika, koja su obezbeđena pravom zaštite podataka EU.

Načelom pravične obrade propisuje se da informacije moraju biti lako razumljive ispitanicima. Mora se upotrebljavati jezik koji odgovara primaocima. Nivo i vrsta upotrebljenog jezika mora se razlikovati u zavisnosti od toga da li su informacije namenjene, na primer, odraslima ili deci, široj javnosti ili stručnim akademskim licima. Pitanje uravnotežavanja aspekta razumljivih informacija razmatra se u Mišljenju Radne grupe iz člana 29. o usklađenijem pružanju informacija. Njime se

535 *Ibid*., član 13. stav 3. i član 14. stav 3.; videti i upućivanje na razumne rokove i izbegavanje nepotrebnog odlaganja na osnovu modernizovane Konvencije br. 108, član 8. stav 1. tačka (b).

536 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 70.

537 Evropska komisija dodatno će razviti informacije koje se prikazuju ikonama i postupke za utvrđivanje standardizovanih ikona putem delegiranih akata; videti Opštu uredbu o zaštiti podataka, član 12. stav 8.

538 Opšta uredba o zaštiti podataka, član 12. st. 1., 5. i 7. i modernizovana Konvencija br. 108, član 9. stav 1. tačka (b).

unapređuje ideja takozvanih „slojevitih obaveštenja"[539] koje ispitaniku omogućavaju da odluči o željenom nivou detalja. Međutim, takvim načinom davanja informacija se rukovalac podacima ne oslobađa obaveze koje ima na osnovu članova 13. i 14. OUZP-a. Rukovalac podacima i dalje je dužan da dâ ispitaniku sve informacije.

Jedan od najefikasnijih načina davanja informacija je postavljanje odgovarajućih informacionih klauzula na naslovnoj strani internet stranice rukovaoca podacima, kao što su pravila zaštite privatnosti internet stranice. Međutim, znatan deo stanovništva ne služi se internetom, što bi društvo ili javni organi trebalo da uzmu u obzir u svojim pravilima informisanja.

Obaveštenje o zaštiti privatnosti, koje se odnosi na obradu ličnih podataka na internet stranici, moglo bi da izgleda kako sledi:

Ko smo mi?

„Rukovalac podacima" jeste kompanija Bed and Breakfast C&U, sa sedištem na adresi [adresa: xxx], tel.: xxx; faks: xxx; e-pošta: info@c&u.com; kontakt podaci službenika za zaštitu podataka: [xxx].

Obaveštenje s informacijama o ličnim podacima čini deo uslova i odredbi kojima su uređene naše hotelske usluge.

Koje podatke prikupljamo od vas?

Od vas prikupljamo sledeće lične podatke: vaše ime, poštansku adresu, telefonski broj, adresu e-pošte, informacije o boravku, broj kreditne i debitne kartice, kao i IP adrese ili nazive domena računara putem kojih ste posetili našu internet stranicu.

Zašto prikupljamo vaše podatke?

Obrađujemo vaše podatke na osnovu vašeg pristanka i u svrhe rezervacija, sklapanja i izvršavanja ugovora u vezi s uslugama koje vam pružamo, kao i radi ispunjavanja svojih zakonskih obaveza, na primer odredbi Zakona o lokalnim

539 Radna grupa iz člana 29. (2004), *Mišljenje 10/2004 o usklađenijem davanju informacija*, WP 100, Bruxelles, 25. novembra 2004.

taksama, prema kojima moramo da prikupljamo lične podatke kako bismo mogli da naplatimo gradski porez za smeštaj.

Kako obrađujemo vaše podatke?

Vaše lične podatke ćemo čuvati tri meseca. Vaši podaci se ne podvrgavaju postupcima automatizovanog donošenja odluka.

Kompanija Bed and Breakfast C&U pridržava se strogih bezbednosnih postupaka kako bi obezbedilo da se vaši lični podaci ne oštete, ne unište i ne otkriju trećoj strani bez vašeg dopuštenja i kako bi se sprečio neovlašćen pristup njima. Računari na kojima se čuvaju informacije smešteni su u bezbedna okruženja s ograničenim fizičkim pristupom. Upotrebljavamo sigurne fajervol sisteme i druge mere za ograničenje elektronskog pristupa. Ako podaci moraju da se prenesu trećoj strani, od nje zahtevamo da ima uspostavljene slične mere za zaštitu vaših ličnih podataka.

Sve informacije koje prikupimo ili evidentiramo ograničene su na naše poslovne prostore. Ličnim podacima smeju da pristupe samo osobe kojima su te informacije nužne za ispunjavanje ugovornih obaveza. Izričito ćemo vas pitati kada su nam potrebne informacije o vašem identitetu. Možda ćemo od vas tražiti da učestvujete u našim sigurnosnim proverama pre nego što vam otkrijemo informacije. Lične podatke koje nam date možete izmeniti u bilo kom trenutku tako da nam se direktno obratite.

Koja su vaša prava?

Imate pravo na pristup svojim podacima, pravo da dobijete primerak svojih podataka, zatražite njihovo brisanje ili ispravku ili zatražite prenos svojih podataka drugom rukovaocu podacima.

Svoje zahteve možete da pošaljete na adresu info@c&u.com. Dužni smo da odgovorimo na vaš zahtev u roku od mesec dana, ali ako je on previše složen ili ako primimo previše drugih zahteva, obavestićemo vas da se taj period može produžiti za dodatna dva meseca.

Pristup vašim ličnim podacima

Imate pravo da pristupite svojim podacima, na zahtev dobijete informacije o razlozima za njihovu obradu, zatražite njihovo brisanje ili ispravku i ne učestvujete u potpuno automatizovanom postupku donošenja odluka bez

uzimanja u obzir vašeg mišljenja. Svoje zahteve možete poslati na adresu info@c&u.com. Takođe imate pravo na prigovor na obradu, pravo da privučete pristanak i podnesete tužbu nacionalnom nadzornom telu ako smatrate da se obradom podataka krši zakon i zatražite odštetu za štetu nastalu zbog nezakonite obrade.

Pravo na podnošenje prigovora/tužbe

OUZP-om se od rukovaoca podacima zahteva da obavesti ispitanike o mehanizmima sprovođenja na osnovu domaćeg prava i prava Unije u slučajevima povrede ličnih podataka. Rukovalac podacima mora da obavesti ispitanike o njihovom pravu na podnošenje prigovora zbog povrede ličnih podataka nadzornom telu ili, po potrebi, tužbe nacionalnom sudu[540]. Pravom Saveta Evrope takođe se propisuje pravo ispitanika na informacije o načinima ostvarivanja njihovih prava, uključujući pravo na pravni lek utvrđeno članom 9. stav 1. tačka (f).

Izuzeća od obaveze obaveštavanja

OUZP-om se utvrđuje izuzeće od obaveze obaveštavanja. U skladu sa članom 13. stav 4. i članom 14. stav 5. OUZP-a, obaveza obaveštavanja ispitanika ne primenjuje se ako oni već imaju sve relevantne informacije[541]. Usto, ako lični podaci nisu dobijeni od ispitanika, obaveza obaveštavanja ne primenjuje se ako je davanje informacija nemoguće ili nesrazmerno, posebno ako se lični podaci obrađuju u svrhe arhiviranja u javnom interesu, u svrhe naučnog ili istorijskog istraživanja ili u statističke svrhe[542].

Zatim, prema OUZP-u, države članice imaju diskreciono ovlašćenje da ograniče obaveze i prava pojedinaca na osnovu Uredbe ako to predstavlja nužnu i srazmernu meru u demokratskom društvu, na primer za zaštitu nacionalne ili javne bezbednosti, odbranu, zaštitu pravosudnih istraga i postupaka ili zaštitu ekonomskih ili finansijskih interesa, kao i privatnih interesa koji su važniji od interesa zaštite podataka[543].

Sva izuzeća ili ograničenja moraju da budu nužna u demokratskom društvu i srazmerna cilju koji nastoji da se ostvari. U vrlo izuzetnim slučajevima, na primer zbog

540 Opšta uredba o zaštiti podataka, član 13. stav 2. tačka (d) i član 14. stav 2. tačka (e); modernizovana Konvencija br. 108, član 8. stav 1. tačka (f).

541 *Ibid.*, član 13. stav 4. i član 14. stav 5. tačka (a).

542 *Ibid.*, član 14. stav 5. tačke od (b) do (e).

543 Opšta uredba o zaštiti podataka, član 23. stav 1.

medicinskih razloga, zaštita ispitanika može da zahteva ograničenje transparentnosti, što se posebno odnosi na ograničenje prava na pristup svakog ispitanika[544]. Međutim, kao minimalni nivo zaštite, domaćim zakonodavstvom mora se poštovati suština osnovnih prava i sloboda zaštićenih pravom Unije[545]. Za to je potrebno da domaće zakonodavstvo sadrži posebne odredbe kojima se objašnjavaju svrha obrade, kategorije obuhvaćenih ličnih podataka, zaštitne mere i drugi procesni zahtevi[546].

Ako se lični podaci prikupljaju u svrhe naučnog ili istorijskog istraživanja ili u statističke svrhe u javnom interesu, pravom Unije ili države članice mogu se predvideti odstupanja od obaveze obaveštavanja ako je verovatno da bi se time moglo onemogućiti ili ozbiljno ugroziti postizanje tih posebnih svrha[547].

Slična ograničenja javljaju se i u okviru prava Saveta Evrope, pa se prava dodeljena ispitanicima na osnovu člana 9. modernizovane Konvencije br. 108 mogu podvrgnuti mogućim ograničenjima iz člana 11. modernizovane Konvencije br. 108 u strogim uslovima. Osim toga, skladno članu 8. stavu 2. modernizovane Konvencije br. 108, obaveza transparentnosti obrade podataka koja se nameće rukovaocima obrade ne primenjuje se ako ispitanik već ima te informacije.

Pravo pojedinca na pristup sopstvenim podacima

Unutar prava Saveta Evrope, pravo pojedinca na pristup sopstvenim podacima izričito je potvrđeno članom 9. modernizovane Konvencije br. 108. Njime se utvrđuje da svaki pojedinac ima pravo na zahtev da dobije informacije o obradi ličnih podataka koji se odnose na njega, i to na razumljiv način. Pravo na pristup nije priznato samo odredbama modernizovane Konvencije br. 108, nego i sudskom praksom ESLJP-a. ESLJP je ponovo tvrdio da pojedinci imaju pravo na pristup informacijama o sopstvenim ličnim podacima i da to pravo proizlazi iz potrebe za poštovanjem privatnog života[548]. Međutim, pravo na pristup ličnim podacima koje čuvaju javne ili privatne organizacije može biti ograničeno u određenim okolnostima[549].

---

544 Opšta uredba o zaštiti podataka, član 15.

545 Opšta uredba o zaštiti podataka, član 23. stav 1.

546 *Ibid*., član 23. stav 2.

547 *Ibid*., član 89. st. 2 i 3.

548 ESLJP, *Gaskin protiv Ujedinjenog Kraljevstva*, br. 10454/83, 7. jula 1989; ESLJP, *Odièvre protiv Francuske* [VV], br. 42326/98, 13. februara 2003; ESLJP, *K. H. i drugi protiv Slovačke*, br. 32881/04, 28. aprila 2009; ESLJP, *Godelli protiv Italije*, br. 33783/09, 25. septembra 2012.

549 ESLJP, *Leander protiv Švedske*, br. 9248/81, 26. marta 1987.

Unutar prava EU, pravo na pristup sopstvenim podacima izričito je potvrđeno u članu 15. OUZP-a, a navedeno je i kao element temeljnog prava na zaštitu ličnih podataka u članu 8. stavu 2. Povelje EU o osnovnim pravima[550]. Pravo pojedinca na pristup sopstvenim ličnim podacima ključni je element evropskog prava zaštite podataka[551].

OUZP-om se propisuje da svaki ispitanik ima pravo na pristup svojim ličnim podacima i na određene informacije o obradi, koje rukovaoci podacima moraju da daju[552]. Svaki ispitanik posebno ima pravo da dobije potvrdu (od rukovaoca podacima) o tome da li se obrađuju njegovi podaci i barem informacije o sledećem:

- svrhama obrade,
- kategorijama ličnih podataka o kojima je reč,
- primaocima ili kategorijama primalaca kojima se lični podaci otkrivaju,
- predviđenom periodu u kojem će lični podaci biti čuvani ili, ako to nije moguće, kriterijumima korišćenima za utvrđivanje tog perioda,
- postojanju prava na ispravku ili brisanje ličnih podataka ili ograničavanje obrade ličnih podataka,
- pravu na podnošenje prigovora nadzornom telu,
- svakoj dostupnoj informaciji o izvoru podataka koji se obrađuju, ako se podaci ne prikupljaju od ispitanika,
- o logici automatizovane obrade podataka u slučaju automatizovanog donošenja odluka.

550 Videti i SPEU, spojeni predmeti C-141/12 i C-372/12, *Y. S. protiv Minister voor Immigratie, Integratie en Asiel i Minister voor Immigratie, Integratie en Asiel protiv M. i S.*, 17. jula 2014; SPEU, C-615/13 P, *ClientEarth i Pesticide Action Network Europe (PAN Europe) protiv Evropske agencije za sigurnost hrane (EFSA) i Evropske komisije*, Evropska komisija, 16. jula 2015.

551 SPEU, spojeni predmeti C-141/12 i C-372/12, *Y. S. protiv Minister voor Immigratie, Integratie en Asiel i Minister voor Immigratie, Integratie en Asiel protiv M. i S.*, 17. jula 2014.

552 Opšta uredba o zaštiti podataka, član 15. stav 1.

Rukovalac podacima mora da dâ ispitaniku kopiju ličnih podataka koji se obrađuju. Sve informacije saopštene ispitaniku moraju da se daju u razumljivom obliku, što znači da rukovalac podacima mora obezbediti da ta osoba razume dobijene informacije. Na primer, navođenje skraćenica iz stručnog žargona, šifrovanih pojmova ili akronima u odgovoru na zahtev za pristup obično nije dovoljan, osim ako se njihovo značenje ne objasni. U slučaju automatizovanog donošenja odluka, uključujući izradu profila, potrebno je objasniti opštu logiku takvog postupka, uključujući kriterijume koji su uzeti u obzir pri ocenjivanju ispitanika. Unutar **prava Saveta Evrope** postoje slične odredbe[553].

Primer: Pristupom sopstvenim ličnim podacima ispitanik može da utvrdi da li su podaci tačni. Zato je neophodno da se ispitanik na razumljiv način obavesti ne samo o ličnim podacima koji se obrađuju, već i o kategorijama u sklopu kojih se oni obrađuju, kao što su ime, IP adresa, geolokacijska koordinata, broj kreditne kartice itd.

Kada podaci nisu prikupljeni od ispitanika, kao odgovor na zahtev za pristup moraju se dati informacije o izvoru podatka ako su dostupne. Ta odredba se mora tumačiti u kontekstu načela pravičnosti, transparentnosti i odgovornosti. Rukovalac podacima ne sme da uništi informacije o izvoru podataka kako bi ih izuzeo od otkrivanja, osim ako bi se brisanje odvilo uprkos prijemu zahteva za pristup, tako da se i dalje mora pridržavati opštih zahteva „odgovornosti".

Kako je utvrđeno sudskom praksom SPEU, pravo na pristup ličnim podacima ne sme se nepotrebno vremenski ograničiti. Ispitanicima takođe treba dati razumnu mogućnost dobijanja informacija o prošlim postupcima obrade podataka.

Primer: U predmetu *Rijkeboer*[554] od SPEU je zatraženo da utvrdi da li može pravo pojedinca na pristup informacijama o primaocima ili kategorijama primalaca ličnih podataka i o sadržaju podataka da se ograniči na godinu dana pre njegovog zahteva za pristup.

553 Vidi modernizovanu Konvenciju br. 108, član 8. stav 1. tačku (c).

554 SPEU, C-553/07, *College van burgemeester en wethouders van Rotterdam protiv M. E. E. Rijkeboer*, 7. maja 2009.

Kako bi utvrdio da li je na osnovu zakonodavstva EU dozvoljeno takvo vremensko ograničenje, SPEU je odlučio da tumači član 12. u kontekstu svrha Direktive. Prvo je istakao da je pravo na pristup nužno kako bi ispitanik mogao da ostvari svoje pravo da rukovalac podacima ispravi, izbriše ili blokira njegove podatke ili obavesti treće strane kojima su podaci otkriveni o toj ispravci, brisanju ili blokiranju. Stvarno pravo na pristup nužno je i kako bi se ispitaniku dala mogućnost da ostvari svoje pravo na prigovor na obradu ličnih podataka ili pravo na podnošenje tužbe i traženje odštete[555].

Radi obezbeđenja praktičnog efekta prava dodeljenih ispitanicima, SPEU je smatrao da se „to pravo mora obavezno odnositi na prošlost. U suprotnom, ispitanik ne bi mogao efikasno da ostvari svoje pravo na ispravku, brisanje ili blokiranje podataka koji se smatraju nezakonitim ili netačnim, odnosno na pokretanje sudskog postupka i naknadu za pretrpljenu štetu".

6.1.2. Pravo na ispravku

Prema pravu EU i **Saveta Evrope**, ispitanici imaju pravo na ispravku svojih ličnih podataka. Tačnost ličnih podataka je ključna za obezbeđenje visokog nivoa zaštite podataka ispitanika[556].

Primer: U predmetu *Ciubotaru protiv Moldavije*[557] podnosilac predstavke nije mogao da promeni upis svog etničkog porekla u službenoj evidenciji s moldavskog na rumunsko navodno zbog toga što nije potkrepio svoj zahtev. ESLJP je smatrao da je prihvatljivo da države zatraže objektivan dokaz pri upisu etničkog porekla pojedinca. Ako se takav zahtev zasniva isključivo na subjektivnim i nepotkrepljenim osnovama, nadležna tela mogu da ga odbiju. Međutim, zahtev podnosioca predstavke nije bio utemeljen samo na subjektivnom poimanju sopstvenog etničkog porekla. On je izneo svoje veze sa rumunskom etničkom grupom koje su mogle objektivno da se provere, na primer jezik, ime, empatija/saosećanje i drugo. Međutim, prema domaćem zakonodavstvu, podnosilac predstavke je morao da obezbedi dokaze da su njegovi roditelji pripadali rumunskoj etničkoj grupi. S obzirom na istorijsku

555 Opšta uredba o zaštiti podataka, član 15. stav 1. tačke (c) i (f), član 16., član 17. stav 2., član 21. i poglavlje VIII.

556 *Ibid*., član 16. i uvodna izjava 65; modernizovana Konvencija br. 108, član 9. stav 1. tačka (e).

557 ESLJP, *Ciubotaru protiv Moldavije*, br. 27138/04, 27. aprila 2010, st. 51 i 59.

situaciju u Moldaviji, takav je zahtev stvorio nepremostivu prepreku upisu etničkog identiteta koji bi se razlikovao od onog upisanog za njegove roditelje koji su zabeležili sovjetski organi. Budući da je podnosiocu predstavke onemogućila postupanje po njegovom zahtevu u kontekstu dokaza koji se mogu objektivno proveriti, država nije ispunila svoju pozitivnu obavezu obezbeđivanja delotvornog poštovanja privatnog života podnosioca predstavke. ESLJP je zato zaključio da je došlo do povrede člana 8. Konvencije.

U nekim slučajevima je dovoljno da ispitanik jednostavno zatraži ispravku, na primer, pravopisne greške u imenu, promenu adrese ili telefonskog broja. U skladom sa **pravom EU** i **Saveta Evrope**, netačni lični podaci moraju da se isprave bez nepotrebnog ili prekomernog odlaganja[558]. Međutim, ako su takvi zahtevi povezani sa pravno značajnim pitanjima, kao što je pravni identitet ispitanika ili mesto prebivališta radi dostave pravnih dokumenata, zahtevi za ispravke možda neće biti dovoljni i rukovalac podacima će moći da zatraži dokaz navodne netačnosti. Takvim zahtevima ispitaniku se ne sme nametnuti nerazuman teret dokaza i tako onemogućiti ispravka njegovih podataka. ESLJP je utvrdio povrede člana 8. EKLJP-a u nekoliko slučajeva u kojima podnosilac predstavke nije mogao da opovrgne tačnost informacija iz tajnih registara[559].

Primer: U predmetu *Cemalettin Canli protiv Turske*[560] ESLJP je utvrdio povredu člana 8. EKLJP-a u netačnom policijskom zveštavanju u krivičnom postupku.

Podnosilac predstavke je dvaput bio podvrgnut krivičnom postupku zbog navodnog članstva u nezakonitim organizacijama, ali nikad nije bio osuđen. Kad je podnosilac predstavke ponovo uhvaćen i optužen za još jedno krivično delo, policija je krivičnom sudu predala izveštaj pod naslovom „*obrazac s informacijama o dodatnim krivičnim delima*", u kojem je podnosilac predstavke bio naveden kao član dveju nezakonitih organizacija. Zahtev podnosioca predstavke za izmenu izveštaja i policijske evidencije bio je neuspešan. ESLJP je smatrao da su informacije u policijskom Izveštaju bile u okviru člana 8. Evropske konvencije o ljudskim pravima, jer bi javne informacije takođe mogle spadati u kategoriju „privatnog života" ako se sistemski prikupljaju i čuvaju u datotekama

558 Opšta uredba o zaštiti podataka, član 16.; modernizovana Konvencija br. 108, član 9. stav 1.

559 ESLJP, *Rotaru protiv Rumunije* [VV], br. 28341/95, 4. maja 2000.

560 ESLJP, *Cemalettin Canli protiv Turske*, br. 22427/04, 18. novembra 2008, st. 33, 42 i 43; ESLJP, *Dalea protiv Francuske,* br. 964/07, 2. februara 2010.

koje čuvaju nadležna tela. Osim toga, policijski izveštaj bio je netačno sastavljen, a njegovo podnošenje krivičnom sudu nije bilo u skladu sa domaćim zakonom. ESLJP je stoga zaključio da je došlo do povrede člana 8. Konvencije.

Tokom građanskog postupka ili postupka pred javnim telom u kojem se odlučuje o tačnosti podataka, ispitanik može zatražiti beleženje naznake ili napomene o osporavanju tačnosti i čekanju službene odluke u svojoj datoteci podataka[561]. U tom periodu rukovalac podacima ne sme da predstavlja podatke kao tačne ili kao izuzete od izmene, naročito trećim stranama.

6.1.3. Pravo na brisanje („pravo na zaborav")

Davanje prava ispitanicima na brisanje sopstvenih podataka posebno je važno za delotvornu primenu načela zaštite podataka, prvenstveno načela smanjenja količine podataka (lični podaci moraju biti ograničeni na ono što je nužno za svrhe u koje se podaci obrađuju). Pravo na brisanje stoga je utvrđeno pravnim instrumentima Saveta Evrope i Evropske unije[562].

Primer: U predmetu *Segerstedt-Wiberg i drugi protiv Švedske*[563] podnosioci su bili povezani s određenim liberalnim i komunističkim političkim strankama. Sumnjali su na to da su informacije o njima unesene u bezbednosnu policijsku evidenciju, pa su zatražili njihovo brisanje. ESLJP je prihvatio činjenicu da je čuvanje predmetnih podataka imalo pravnu osnovu i legitimnu svrhu. Međutim, u pogledu nekih podnosilaca predstavki ESLJP je utvrdio da je kontinuirano zadržavanje podataka predstavljalo nesrazmerno mešanje u njihove privatne živote. Na primer, u slučaju jednog podnosioca predstavke, nadležna tela su zadržala informaciju da je 1969. godine navodno zagovarao nasilan otpor policijskoj kontroli tokom demonstracija. ESLJP je utvrdio da te informacije nisu mogle da budu ni u kakvom interesu nacionalne bezbednosti, naročito s obzirom na to da se odnose na prošlost. ESLJP je zaključio da je povređen član 8. Konvencije u pogledu četvorice od petorice podnosilaca predstavki, budući da dalje zadržavanje njihovih podataka nije bilo korisno zbog dugog perioda koji je protekao od navodnih dela koja su učinili.

561 Opšta uredba o zaštiti podataka, član 18. i uvodna izjava 67.

562 *Ibid*., član 17.

563 ESLJP, *Segerstedt-Wiberg i drugi protiv Švedske*, br. 62332/00, 6. juna 2006, st. 89 i 90; na primer, videti i ESLJP, *M. K. protiv Francuske*, br. 19522/09, 18. aprila 2013.

Primer: U predmetu *Brunet protiv Francuske*[564] podnosilac predstavke je prijavio čuvanje njegovih ličnih podataka u policijskoj bazi podataka koja je sadržala informacije o osuđenim licima, optuženicima i žrtvama. Iako je krivični postupak protiv podnosioca predstavke obustavljen, njegovi podaci su bili navedeni u bazi podataka. ESLJP je zaključio da je došlo do povrede člana 8. Konvencije. Prilikom donošenja odluke ESLJP je smatrao da u praksi nije postojala mogućnost da podnosilac predstavke izbriše svoje lične podatke iz baze podataka. ESLJP je takođe razmotrio prirodu informacija uvršćenih u bazu podataka i zaključio da se time narušava privatnost podnosioca predstavke, jer su one sadržale pojedinosti o njegovom identitetu i ličnosti. Usto, zaključio je da je period zadržavanja lične evidencije u bazi podataka, koji je trajao 20 godina, bio predug, naročito zato što podnosilac predstavke nikada nije bio osuđivan.

U modernizovanoj Konvenciji br. 108 izričito se potvrđuje da svaki pojedinac ima pravo na brisanje netačnih, pogrešnih ili nezakonito obrađenih podataka[565].

U okviru prava EU, članom 17. OUZP-a utvrđuje se pravo ispitanika na brisanje podataka. Pravo na brisanje ličnih podataka bez nepotrebnog odgađanja primenjuje se:

- ako lični podaci više nisu nužni u odnosu na svrhe za koje su prikupljeni ili na drugi način obrađeni,
- ako ispitanik povuče pristanak na kome se obrada zasniva i ako ne postoji druga pravna osnova za obradu,
- ako ispitanik uloži prigovor na obradu i ne postoje jači legitimni razlozi za obradu,
- ako su lični podaci nezakonito obrađeni,
- ako lični podaci moraju da se brišu radi poštovanja pravne obaveze iz prava Unije ili države članice kojem podleže rukovalac podacima,
- ako su lični podaci prikupljeni u vezi sa ponudom usluga informatičke kompanije deci u skladu sa članom 8. OUZP-a[566].

564 ESLJP, *Brunet protiv Francuske*, br. 21010/10, 18. septembra 2014.

565 Modernizovana Konvencija br. 108, član 9. stav 1. tačka (e).

566 Opšta uredba o zaštiti podataka, član 17. stav 1.

Teret dokazivanja da je obrada podataka zakonita snose rukovaoci podacima, jer su oni odgovorni za zakonitost obrade[567]. Prema načelu odgovornosti, rukovalac podacima mora u svakom trenutku biti u mogućnosti da dokaže da postoji čvrsta pravna osnova za obradu podataka. U suprotnom se obrada mora prekinuti[568]. OUZP-om se definišu izuzeća od prava na zaborav, uključujući slučajeve u kojima je obrada ličnih podataka nužna:

- radi ostvarivanja prava na slobodu izražavanja i informisanja,
- radi poštovanja pravne obaveze kojom se zahteva obrada prema pravu Unije ili pravu države članice kojem podleže rukovalac podacima ili za izvršavanje zadatka od javnog interesa ili pri izvršavanju službenog ovlašćenja rukovaoca podacima,
- zbog javnog interesa u oblasti javnog zdravlja,
- u svrhe arhiviranja u javnom interesu, u svrhe naučnog ili istorijskog istraživanja ili u statističke svrhe,
- radi postavljanja, ostvarivanja ili odbrane pravnih zahteva[569].

SPEU je potvrdio važnost prava na brisanje za obezbeđivanje visokog nivoa zaštite podataka.

Primer: U predmetu *Google Spain*[570] SPEU je razmatrao je li kompanija Gugl bila obavezana da izbriše zastarele informacije o finansijskim poteškoćama tužioca iz popisa rezultata pretraživanja. Između ostalog, kompanija Google osporavala je svoju odgovornost, tvrdeći da ona daje samo link na internet stranici izdavača na kojoj se nalaze informacije, u ovom slučaju stranicu novina koje su objavile

567 Ibid.

568 *Ibid.*, član 5. stav 2.

569 *Ibid.*, član 17. stav 3.

570 SPEU, C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje Gonzáleza* [VV], 13. maja 2014., st. od 55 do 58.

članak o stečaju tužioca[571]. Gugl je tvrdio da zahtev za brisanje zastarelih informacija s internet stranice treba uputiti vlasniku internet stranice, a ne kompaniji Gugl, koja samo daje link za izvornu stranicu. SPEU je zaključio da kompanija Gugl prilikom pretraživanja informacija i internet stranica na internetu, kao i indeksiranja sadržaja radi pokazivanja rezultata pretraživanja postaje rukovalac podacima na kojeg se primenjuju odgovornosti i obaveze na osnovu prava Unije.

SPEU je pojasnio da internet pretraživači i rezultati pretraživanja koji sadrže lične podatke mogu poslužiti za izradu detaljnog profila osobe[572]. Internet pretraživači čine informacije sadržane u takvom popisu široko dostupnima. Uzimajući u obzir moguću ozbiljnost mešanja, ono se ne može opravdati samo ekonomskim interesom koji administrator pretraživača ima u takvoj obradi. Mora se nastojati da se postigne pravična ravnoteža između legitimnog interesa korisnika interneta za pristup informacijama i osnovnih prava ispitanika prema članovima 7. i 8. Povelje EU o osnovnim pravima. U društvu koje postaje sve više digitalizovano, zahtev da lični podaci budu tačni i da ne prelaze ono što je nužno (odnosno javne informacije) ključan je za obezbeđivanje visokog nivoa zaštite podataka pojedinaca. „[N]adzornik u okviru svojih odgovornosti, nadležnosti i mogućnosti [mora] da obezbedi da ta aktivnost zadovoljava uslove" iz prava Unije kako bi utvrđene pravne garancije mogle da razviju svoj puni učinak[573]. To znači da pravo na brisanje sopstvenih ličnih podataka kada je obrada zastarela ili više nije potrebna, takođe, obuhvata rukovaoce podacima koji repliciraju informacije[574].

---

571 Gugl je takođe osporio primenu propisa EU o zaštiti podataka zbog činjenice da kompanija Gugl ima sedište u SAD i da se predmetna obrada ličnih podataka takođe odvijala u SAD. Drugi argument protiv primene zakonodavstva EU o zaštiti podataka odnosio se na tvrdnju da se internet pretraživači ne mogu smatrati „rukovaocima podacima" u pogledu podataka koji se prikazuju u njihovim rezultatima jer nemaju saznanja o tim podacima niti ih kontrolišu. SPEU je odbacio oba argumenta, tvrdeći da je Direktiva 95/46/EZ primenjiva u tom slučaju, pa je nastavio da razmatra oblast primene prava koja su njome zajamčena, a posebno prava na brisanje ličnih podataka.

572 *Ibid*., st. 36, 38, 80, 81 i 97.

573 *Ibid*., st. od 81 do 83.

574 SPEU, C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González* [VV], 13. maja 2014., st. 88. Vidi i Radna grupa iz člana 29. (2014), *Guidelines on the implementation of the CJEU judgment on „Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González"* C-131/12 (Smernice o izvršenju presude Suda Evropske unije u predmetu *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González*, C-131/12), WP 225, Bruxelles, 26. novembra 2014. i Preporuku CM/Rec 2012(3) Saveta ministara državama članicama o zaštiti ljudskih prava u pogledu internet pretraživača, 4. aprila 2012.

Prilikom razmatranja da li je Gugl obavezan da ukloni linkove povezane sa tužiocem SPEU je zaključio da u određenim uslovima pojedinci imaju pravo da zatraže brisanje svojih ličnih podataka. Na to pravo se može pozvati kada informacije o nekom pojedincu nisu tačne, dovoljne ili relevantne ili ih je previše za svrhe obrade podataka. SPEU je potvrdio da to pravo nije apsolutno, nego se mora proceniti u odnosu na druga prava i interese, naročito interes šire javnosti na pristup određenim informacijama. Svaki zahtev za brisanje mora se proceniti pojedinačno kako bi se uspostavila ravnoteža između osnovnih prava na zaštitu ličnih podataka i privatni život ispitanika, s jedne strane, i legitimnih interesa svih korisnika interneta, uključujući izdavače, s druge. SPEU je pružio smernice o činiocima koje je potrebno razmotriti prilikom procenjivanja interesa. Priroda tih informacija posebno je važan činilac. Ako su informacije u vezi sa privatnim životom pojedinca i ne postoji javni interes za dostupnošću tih informacija, zaštita podataka i privatnost bile bi važnije od prava šire javnosti na pristup informacijama. Sa druge strane, ako je ispitanik javna ličnost ili priroda informacija opravdava njihovo stavljanje na raspolaganje široj javnosti, prevladavajući interes šire javnosti za pristup informacijama može biti opravdanje za mešanje u osnovna prava na zaštitu podataka i privatnost ispitanika.

Sledom te presude, Radna grupa iz člana 29. usvojila je smernice o sprovođenju odluke SPEU[575]. Smernice sadrže popis uobičajenih merila koje nadzorna tela mogu da upotrebe prilikom obrade tužbi u vezi sa zahtevima pojedinaca za brisanje, objašnjenja toga što pravo na brisanje podrazumeva i vođenja osoba kroz postupak uravnotežavanja prava. U smernicama se ponavlja da se procene moraju sprovesti pojedinačno za svaki slučaj. Budući da pravo na zaborav nije apsolutno, ishod zahteva može se razlikovati od slučaja do slučaja. To je vidljivo i u sudskoj praksi SPEU nakon presude u predmetu Gugl.

Primer: U predmetu *Camera di Commercio di Lecce protiv Mannija*[576] SPEU je morao da istraži da li je pojedinac imao pravo na brisanje svojih ličnih podataka objavljenih u javnom registru trgovačkih kompanija nakon što je njegova trgovačka kompanija prestala da postoji. G. Mani je zatražio od Ekonomske komore grada Leće u Italiji da izbriše njegove lične podatke iz tog registra nakon

575 Radna grupa iz člana 29. (2014), *Smernice o izvršenju presude Suda Evropske unije u predmetu Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González*, C-131/12, WP 225, Bruxelles, 26. novembra 2014.

576 SPEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce protiv Salvatorea Mannija*, 9. marta 2017.

što je otkrio da bi potencijalni klijenti pretraživali registar i saznali da je nekada bio direktor kompanije koja je proglasila stečaj pre više od decenije. Tužilac je smatrao da bi te informacije odvratile potencijalne klijente.

Prilikom procene prava g. Manija na zaštitu njegovih ličnih podataka s interesom šire javnosti za pristup tim informacijama, SPEU je prvo razmotrio svrhu javnog registra. Istakao je činjenicu da je objava podataka propisana zakonom, a naročito direktivom EU kojoj je svrha da učini podatke o društvima dostupnijima trećim stranama. Treće strane tako bi ostvarile pristup i mogle da prouče osnovnu dokumentaciju i druge informacije o određenoj kompaniji, „posebno pojedinosti o licima koja su ovlašćena da obavežu trgovačku kompaniju". Svrha otkrivanja bila je takođe da se garantuje pravna sigurnost s obzirom na jačanje trgovine među državama članicama, obezbeđujući da treće strane imaju pristup svim relevantnim informacijama o kompanijama u celoj EU.

SPEU je takođe napomenuo da prava i zakonske odredbe kompanije često nastavljaju da važe i posle određenog vremena, čak i nakon likvidacije kompanije. Sporovi u vezi sa likvidacijom mogu se odužiti, a pitanja o kompaniji, njenim direktorima i stečajnim upravnicima mogu se postaviti i godinama nakon prestanka njenog postojanja. SPEU je smatrao da se, s obzirom na brojne moguće scenarije i raznolikost rokova zastare propisanih u pojedinim državama članicama, „čini [...] da je u ovom trenutku nemoguće utvrditi jedinstveni rok, koji počinje da teče od prestanka kompanije, po čijem isteku upis navedenih podataka u registru i njihovo objavljivanje više nije potrebno". Zbog legitimnog cilja otkrivanja podataka i poteškoća u utvrđivanju perioda po čijem isteku bi lični podaci mogli da se izbrišu iz registra bez ugrožavanja interesa trećih strana, SPEU je zaključio da se pravilima EU o zaštiti podataka ne garantuje pravo na brisanje ličnih podataka za lica koja se nađu u situaciji g. Manija.

Kada rukovalac podacima učini lične podatke javno dostupnima, pa potom mora da ih izbriše, dužan je i mora da preduzme odgovarajuće korake kako bi obavestio druge rukovaoce podacima koji obrađuju iste podatke o zahtevu za brisanje ispitanika. Aktivnosti rukovaoca podacima moraju da se zasnivaju na dostupnim tehnologijama i troškovima izvršenja[577].

577 Opšta uredba o zaštiti podataka, član 17. stav 2. i uvodna izjava 66.

6.1.4. Pravo na ograničenje obrade

Članom 18. OUZP-a ispitanicima se omogućava da privremeno ograniče obradu svojih ličnih podataka koju vrši rukovalac podacima. Ispitanici mogu zatražiti od rukovaoca podacima da ograniči obradu kada [se]::

- osporava tačnost ličnih podataka,
- je obrada nezakonita i ispitanik traži ograničenje upotrebe ličnih podataka umesto njihovog brisanja,
- podaci moraju čuvati radi ostvarivanja ili odbrane pravnih zahteva,
- očekuje odluka o tome da li legitimni interesi rukovaoca podacima nadilaze interese ispitanika[578].

Metode kojima rukovalac podacima može ograničiti obradu ličnih podataka mogu uključivati, na primer, privremeno premeštanje odabranih ličnih podataka u drugi sistem obrade, činjenje odabranih podataka nedostupnima za korisnike ili privremeno uklanjanje ličnih podataka[579]. Rukovalac podacima mora da obavesti ispitanika pre nego što ograničenje obrade bude ukinuto[580].

Obaveza izveštavanja u vezi s ispravkom ili brisanjem ličnih podataka ili ograničenjem obrade

Rukovalac podacima mora da objavi svaku ispravku ili brisanje ličnih podataka ili ograničenje obrade svakom primaocu kome su otkriveni lični podaci, osim ako se to pokaže nemogućim ili zahteva nesrazmeran napor[581]. Ako ispitanik zatraži informacije o tim primaocima, rukovalac podacima mora da mu ih dâ[582].

6.1.5. Pravo na prenosivost podataka

Prema OUZP-u, ispitanici imaju pravo na prenosivost podataka u situacijama u kojima se lični podaci koje daju rukovaocu podacima obrađuju automatizovanim

578 *Ibid*., član 18. stav 1.
579 *Ibid*., uvodna izjava 67.
580 *Ibid*., član 18. stav 3.
581 *Ibid.*, član 19.
582 *Ibid.*

putem na osnovu pristanka ili kada je obrada ličnih podataka nužna za izvršenje ugovora i sprovodi se automatizovanim putem. To znači da se pravo na prenosivost podataka ne primenjuje u slučajevima u kojima se obrada ličnih podataka zasniva na pravnoj osnovi koja nije pristanak ili ugovor[583].

Ako se pravo na prenosivost podataka primenjuje, ispitanici imaju pravo na neposredni prenos ličnih podataka od jednog rukovaoca podacima drugom ako je to tehnički izvodljivo[584]. Da bi to olakšao, rukovalac podacima treba da razvije interoperabilne formate kojima se ispitanicima omogućava prenosivost podataka[585]. OUZP-om se utvrđuje da ti formati moraju da budu strukturirani, uobičajeno upotrebljavani i otvoreni kako bi se olakšala interoperabilnost[586]. Interoperabilnost se u širem smislu može definisati kao sposobnost informacionih sistema da razmenjuju podatke i omogućavaju deljenje informacija[587]. Iako je svrha formata koji se koriste postizanje interoperabilnosti, u OUZP-u se ne navode konkretne preporuke u pogledu posebnih formata; oni se mogu razlikovati od sektora do sektora[588].

Prema Smernicama Radne grupe iz člana 29., pravom na prenosivost podataka „podržavaju [se] korisnički izbor, kontrola i osnaživanje korisnika" kako bi ispitanici preuzeli kontrolu nad svojim ličnim podacima[589]. U smernicama se opisuju glavni elementi prenosivosti podataka, koji uključuju:

- pravo ispitanika da dobiju sopstvene lične podatke koje je obradio rukovalac podacima u strukturiranom, uobičajeno upotrebljavanom, otvorenom i interoperabilnom formatu,

- pravo prenosa ličnih podataka od jednog rukovaoca podacima drugom bez ometanja ako je to tehnički izvodljivo,

- režim kontrole: kada rukovalac podacima odgovara na zahtev za prenosivost podataka, deluje prema uputstvima ispitanika, što znači da nije odgovoran za

583 *Ibid*., uvodna izjava 68 i član 20. stav 1.

584 *Ibid*., član 20. stav 2.

585 *Ibid*., uvodna izjava 68 i član 20. stav 1.

586 *Ibid*., uvodna izjava 68.

587 Evropska komisija, Komunikacija „Jači i pametniji informatički sistemi za granice i bezbednost", COM(2016) 205 final, 2. aprila 2016.

588 Radna grupa iz člana 29. (2016), Smernice o pravu na prenosivost podataka, WP 242, 13. decembra 2016, revidirane 5. aprila 2017, str. 17–18.

589 *Ibid*.

usklađenost primaoca s pravom zaštite podataka jer ispitanik odlučuje kome se podaci prenose,

- ostvarivanje prava na prenosivost podataka bez dovođenja bilo kog drugog prava u pitanje, što važi i za druga prava iz OUZP-a.

6.1.6. Pravo na prigovor

Ispitanici imaju pravo da ulože prigovor na obradu ličnih podataka na osnovu svoje posebne situacije, kao i podataka koji se obrađuju za potrebe neposrednog marketinga. Pravo na prigovor može se ostvariti automatizovanim putem.

Pravo na prigovor na osnovu posebne situacije ispitanika

Ne postoji opšte pravo ispitanika na prigovor na obradu njihovih podataka[590]. Članom 21. stav 1. OUZP-a ispitanicima se daje pravo da ulože prigovor na osnovu svoje posebne situacije ako je pravna osnova obrade ispunjavanje zadatka rukovaoca podacima u javnom interesu ili ako se obrada zasniva na legitimnim interesima rukovaoca podacima[591]. Pravo na prigovor primenjuje se na aktivnosti izrade profila. Slično pravo potvrđeno je i modernizovanom Konvencijom br. 108[592].

Cilj prava na prigovor na osnovu posebne situacije ispitanika jeste da se postigne odgovarajuća ravnoteža između prava ispitanika na zaštitu podataka i legitimnih prava drugih u postupku obrade njihovih podataka. Međutim, SPEU je pojasnio da prava ispitanika generalno imaju nadmoć nad ekonomskim interesima rukovaoca podacima u zavisnosti od „prirode informacije o kojoj je reč, o njenoj osetljivosti u odnosu na privatnost osobe čiji se podaci obrađuju, kao i o javnom interesu za tu informaciju"[593]. U skladu sa OUZP-om, teret dokazivanja snose rukovaoci podacima, koji moraju da dokažu da postoje uverljivi razlozi za nastavak obrade[594]. Isto tako, u Izveštaju s objašnjenjima o modernizovanoj Konvenciji br. 108 pojašnjava se da se

590 Vidi i ESLJP, *M. S. protiv Švedske*, br. 20837/92, 27. avgusta 1997. (predmet u kome su medicinski podaci objavljeni bez pristanka ili mogućnosti prigovora); ESLJP, *Leander protiv Švedske*, br. 9248/81, 26. marta 1987; ESLJP, *Mosley protiv Ujedinjenog Kraljevstva*, br. 48009/08, 10. maja 2011.

591 Opšta uredba o zaštiti podataka, uvodna izjava 69; član 6. stav 1. tačke (e) i (f).

592 Modernizovana Konvencija br. 108, član 9. stav 1. tačka (d); Preporuka o izradi profila, član 5. stav 3.

593 SPEU, C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje Gonzáleza* [VV], 13. maja 2014, stav 81.

594 Vidi i modernizovanu Konvenciju br. 108, član 98. stav 1. tačka (d) u kojoj stoji da ispitanik može da uloži prigovor na obradu svojih podatka, „osim ako rukovalac podacima ne dokaže legitimne razloge za obradu koji imaju nadmoć nad njegovim interesima ili pravima i osnovnim slobodama".

legitimni razlozi za obradu podataka (koji mogu da prevagnu nad pravom ispitanika na prigovor) moraju dokazivati za svaki pojedini slučaj[595].

Primer: U predmetu *Manni*[596] SPEU je smatrao da zbog legitimne svrhe otkrivanja ličnih podataka u registru trgovačkih kompanija, a naročito potrebe za zaštitom interesa trećih strana i obezbeđivanja pravne sigurnosti, g. Mani u načelu nije imao pravo na brisanje svojih ličnih podataka iz registra. Međutim, potvrdio je da postoji pravo na prigovor na obradu, navodeći da „se ne može isključiti mogućnost postojanja određenih situacija u kojima jaki i zakoniti razlozi u vezi sa konkretnim slučajem predmetnog lica izuzetno opravdavaju ograničavanje pristupa ličnim podacima koji se na nju odnose, upisanih u registar, po isteku dovoljno dugog roka [...] trećim osobama koje imaju konkretan interes za uvid u njih".

SPEU je smatrao da su domaći sudovi odgovorni za procenu svakog predmeta, uzimajući u obzir sve pojedinačne relevantne okolnosti i moguće postojanje legitimnih i jakih razloga kojima bi se izuzetno mogao opravdati ograničen pristup trećih strana ličnim podacima sadržanima u registrima trgovačkih kompanija. Međutim, obrazložio je da se u slučaju g. Manija činjenica da je otkrivanje njegovih ličnih podataka u registru navodno uticalo na njegove klijente sama po sebi ne može smatrati takvim legitimnim i preovlađujućim razlogom. Potencijalni klijenti g. Manija imaju legitiman interes za pristup informacijama o stečaju njegove prethodne kompanije.

Rezultat uspešnog prigovora je da rukovalac podacima više ne može da obrađuje predmetne podatke. Međutim, postupci obrade podataka ispitanika pre prigovora ostaju legitimni.

Pravo na prigovor na obradu podataka u svrhu ciljanog marketinga

Članom 21. stav 2. OUZP-a utvrđuje se posebno pravo na prigovor na upotrebu ličnih podataka za potrebe ciljanog marketinga, čime se dodatno pojašnjava član 13. Direktive o privatnosti i elektronskim komunikacijama. To pravo je utvrđeno i u modernizovanoj Konvenciji br. 108, kao i u Preporuci o neposrednom marketingu Saveta

595 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 78.

596 SPEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce protiv Salvatorea Mannija*, 9. marta 2017, st. 47 i 60.

Evrope[597]. U Izveštaju s objašnjenjima o modernizovanoj Konvenciji br. 108 pojašnjava se da prigovori na obradu podataka za potrebe ciljanog marketinga treba da dovedu do bezuslovnog brisanja ili uklanjanja predmetnih ličnih podataka[598].

Ispitanik ima pravo na prigovor na upotrebu njegovih ličnih podataka u svrhe ciljanog marketinga, bez naplate i u bilo kom trenutku. Ispitanici moraju da budu jasno obavešteni o tom pravu, nezavisno od svih drugih informacija.

Pravo na prigovor automatizovanim putem

Kada se lični podaci upotrebljavaju i obrađuju za usluge informatičke kompanije, ispitanik može da iskoristi svoje pravo na prigovor na obradu svojih ličnih podataka automatizovanim putem.

Usluge informatičke kompanije definišu se kao svaka usluga koja se obično pruža uz naknadu, na daljinu, elektronskim sredstvima, kao i na lični zahtev primaoca usluga[599].

Rukovaoci podacima koji pružaju usluge informatičke kompanije moraju da uspostave odgovarajuće tehničke mere i postupke kako bi obezbedili da se pravo na prigovor automatizovanim putem može delotvorno ostvariti[600]. Na primer, to može uključivati blokiranje kolačića na internet stranicama ili isključivanje funkcije praćenja pri pretraživanju interneta.

Pravo na prigovor u svrhe naučnog ili istorijskog istraživanja ili u statističke svrhe

U skladu sa pravom EU, naučno istraživanje treba da se tumači u širokom smislu, uključujući na primer tehnološki razvoj i demonstracione aktivnosti, temeljno istraživanje, primenjeno istraživanje, kao i istraživanje koje se finansira iz privatnih izvora[601]. Istorijsko istraživanje takođe uključuje istraživanje u genealoške svrhe,

597 Savet Evrope, Savet ministara (1985.), Preporuka Rec(85)20 državama članicama o zaštiti ličnih podataka koji se koriste u svrhu neposrednog marketinga, 25. oktobra 1985, član 4. stav 1.

598 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 79.

599 Direktiva 98/34/EZ kako je izmenjena Direktivom 98/48/EZ o utvrđivanju postupka pružanja informacija u oblasti tehničkih normi i propisa, član 1. stav 2.

600 Opšta uredba o zaštiti podataka, član 21. stav 5.

601 *Ibid*., uvodna izjava 159.

imajući u vidu da Uredba ne bi trebalo da se primenjuje na preminule osobe[602]. Statističke svrhe znače svako prikupljanje i obradu ličnih podataka potrebnih za statistička istraživanja ili za proizvodnju statističkih rezultata[603]. I ovde je posebna situacija ispitanika pravna osnova za pravo na prigovor na obradu ličnih podataka u svrhe istraživanja[604]. Jedini izuzetak je nužnost obrade za izvršavanje zadatka zbog javnog interesa. Međutim, pravo na brisanje ne primenjuje se kada je obrada nužna (nezavisno od postojanja javnog interesa) u svrhe naučnog ili istorijskog istraživanja ili u statističke svrhe[605].

U OUZP-u se uspostavlja ravnoteža između zahteva naučnog, statističkog ili istorijskog istraživanja i prava ispitanika pomoću posebnih zaštitnih mera i odstupanja iz člana 89. Stoga se pravom Unije ili države članice mogu propisati odstupanja od prava na prigovor u meri u kojoj je verovatno da bi takvo pravo onemogućilo ili znatno ugrozilo ispunjenje istraživačkih svrha, ako su takva odstupanja nužna za ispunjenje tih svrha.

Unutar **prava Saveta Evrope**, članom 9. stav 2. modernizovane Konvencije br. 108 utvrđuje se da se ograničenja prava ispitanika, uključujući pravo na prigovor, mogu propisati zakonom o obradi podataka u svrhe arhiviranja u javnom interesu, u svrhe naučnog ili istorijskog istraživanja ili u statističke svrhe, ako ne postoji jasan rizik kršenja prava i osnovnih sloboda ispitanika.

Međutim, u Izveštaju s objašnjenjima (stav 41) takođe se utvrđuje da ispitanici treba da imaju mogućnost da daju pristanak samo za određene oblasti istraživanja ili delove istraživačkih projekata u meri u kojoj to predviđena svrha dopušta i da ulože prigovor ako smatraju da se obradom prekomerno narušavaju njihova prava i slobode bez legitimne osnove.

Drugim rečima, takva obrada bi se unapred smatrala usklađenom pod uslovom da postoje druge zaštitne mere i da se u tim postupcima u načelu izuzima svaka upotreba informacija prikupljenih za donošenje odluka ili mera o određenom pojedincu.

602 *Ibid.*, uvodna izjava 160.

603 *Ibid.*, uvodna izjava 162.

604 *Ibid.*, član 21. stav 6.

605 *Ibid.*, član 17. stav 3. tačka (d).

6.1.7. Automatizovano pojedinačno donošenje odluka, uključujući izradu profila

Automatizovane odluke jesu odluke donesene na osnovu ličnih podataka obrađenih isključivo automatizovanim putem, bez ljudske intervencije. **Prema pravu EU**, ispitanici ne smeju da budu podvrgnuti automatizovanim odlukama koje imaju pravni ili sličan učinak. Ako je za takve odluke verovatno da će znatno uticati na živote pojedinaca jer se odnose, na primer, na kreditnu sposobnost, zapošljavanje putem interneta, učinak na poslu ili analizu ponašanja ili pouzdanosti, nužna je posebna zaštita radi izbegavanja negativnih posledica. Automatizovano donošenje odluka uključuje izradu profila koja se sastoji od svakog oblika automatske procene „ličnih aspekata povezanih s pojedincem, posebno za analizu ili predviđanje aspekata u vezi s radnim učinkom, ekonomskim stanjem, zdravljem, ličnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog pojedinca”[606].

Primer: Radi brze procene kreditne sposobnosti budućeg klijenta, agencije za kreditni rejting (CRA) prikupljaju određene podatke, kao što su način na koji je klijent održavao svoj kreditni račun i uslužne/komunalne račune, pojedinosti o njegovim prethodnim adresama, kao i informacije iz javnih izvora poput popisa birača, javnih evidencija (uključujući sudske presude) ili podataka o bankrotu ili insolventnosti. Ti lični podaci se potom učitavaju u algoritam za procenjivanje koji izračunava ukupnu vrednost koja predstavlja kreditnu sposobnost potencijalnog klijenta.

Prema Radnoj grupi iz člana 29., pravo da se na pojedinca ne odnose odluke koje se zasnivaju isključivo na automatizovanoj obradi koje mogu da proizvedu pravne efekte za ispitanika ili koje znatno na njega utiču jednako je opštoj zabrani i ne zahteva da ispitanik proaktivno uloži prigovor na takvu odluku[607].

Ipak, u skladu sa OUZP-om, automatizovano donošenje odluka koje proizvode pravne učinke ili značajno utiču na pojedince može biti prihvatljivo ako je nužno za sklapanje ili izvršenje ugovora između rukovaoca podacima i ispitanika ili ako ispitanik da izričiti pristanak. Automatizovano donošenje odluka takođe je prihvatljivo

606 *Ibid*., uvodna izjava 71., član 4. stav 4. i član 22.

607 Radna grupa iz člana 29., Smernice o automatiziranom pojedinačnom donošenju odluka i izradi profila za potrebe Uredbe 2016/679, WP 251, 3. oktobra 2017., str. 15.

ako je dozvoljeno zakonom i ako su prava, slobode i legitimni interesi ispitanika odgovarajuće zaštićeni[608].

Među obavezama rukovaoca podacima u vezi s informacijama koje treba dati prilikom prikupljanja ličnih podataka, OUZP-om se propisuje i da ispitanici moraju da budu obavešteni o postojanju automatizovanog donošenja odluka, uključujući izradu profila[609]. To ne utiče na pravo na pristup ličnim podacima koje obrađuje rukovalac podacima[610]. Informacije ne bi trebalo da upućuju samo na činjenicu da će se izraditi profil, već bi trebalo da sadrže i smislene informacije o logici na kojoj se izrada profila zasniva, kao i predviđenim posledicama takve obrade za pojedince[611]. Na primer, društvo za zdravstveno osiguranje koje upotrebljava automatizovano donošenje odluka o zahtevima treba ispitanicima da dâ opšte informacije o načinu rada algoritma i činiocima pomoću kojih algoritam izračunava njihove premije osiguranja. Isto tako, prilikom ostvarivanja „prava na pristup" ispitanici mogu da zatraže informacije od rukovaoca podacima o postojanju automatizovanog donošenja odluka i smislene informacije o tome o kojoj je logici reč[612].

Svrha informacija datih ispitanicima jeste da se obezbedi transparentnost i omogući ispitanicima da daju pristanak zasnovan na informacijama, ako je potreban, ili da ostvare pravo na ljudsku intervenciju. Rukovalac podacima mora sprovesti odgovarajuće mere za zaštitu prava, sloboda i legitimnih interesa ispitanika. To uključuje barem pravo na ljudsku intervenciju rukovaoca podacima i mogućnost da ispitanik izrazi sopstveni stav i ospori odluku na osnovu automatizovane obrade svojih ličnih podataka[613].

Radna grupa iz člana 29. izradila je dodatne smernice o upotrebi automatizovanog donošenja odluka na osnovu OUZP-a[614].

Prema pravu Saveta Evrope, pojedinci imaju pravo na to da se o njima ne donose odluke koje značajno utiču na njih ili koje se zasnivaju isključivo na automatizovanoj

608 Opšta uredba o zaštiti podataka, član 22. stav 2.

609 *Ibid*., član 12.

610 *Ibid*., član 15.

611 *Ibid*., član 13. stav 2. tačka (f).

612 *Ibid*., član 15. stav 1. tačka (h).

613 *Ibid*., član 22. stav 3.

614 Radna grupa iz člana 29. (2017), *Smernice o automatizovanom pojedinačnom donošenju odluka i izradi profila za potrebe Uredbe 2016/679,* WP 251, 3. oktobra 2017.

obradi bez uzimanja u obzir njegovog mišljenja[615]. Zahtev za uzimanje u obzir mišljenja ispitanika kada se odluke zasnivaju isključivo na automatizovanoj obradi podrazumeva da on ima pravo da ospori takve odluke, kao i da bi trebalo da ima mogućnost da ospori svaku netačnost ličnih podataka koje rukovalac podacima upotrebljava i relevantnost bilo kojeg profila koji se na nju primenjuje[616]. Međutim, pojedinac ne može ostvariti to pravo ako je automatizovana odluka dozvoljena zakonom kojem rukovalac podacima podleže i kojim se uspostavljaju odgovarajuće mere za zaštitu prava, sloboda i legitimnih interesa ispitanika. Usto, ispitanici imaju pravo na zahtev da dobiju informacije o razlozima za obradu podataka koja se vrši[617]. U Izveštaju sa objašnjenjima o modernizovanoj Konvenciji br. 108 navodi se primer određivanja kreditne sposobnosti. Pojedinci bi trebalo da imaju pravo da saznaju ne samo za pozitivnu ili negativnu odluku o kreditnoj sposobnosti, nego i za *logiku* na kojoj se zasniva obrada njihovih ličnih podataka koja je dovela do takve odluke. „Razumevanje tih elemenata doprinosi delotvornom izvršenju drugih ključnih zaštitnih mera, kao što su pravo na prigovor i pravo na tužbu nadležnom telu"[618].

Iako nije pravno obavezujuća, u Preporuci o profilisanju utvrđuju se uslovi prikupljanja i obrade ličnih podataka u kontekstu izrade profila[619]. Ona sadrži odredbe o potrebi da se obezbedi da obrada u kontekstu izrade profila bude pravična, zakonita, proporcionalna i služi utvrđenim i legitimnim svrhama. Takođe sadrži odredbe o informacijama koje rukovaoci podacima treba da daju ispitanicima. U Preporuci je utvrđeno i načelo kvaliteta podataka, prema kojem rukovaoci podacima moraju da preduzmu mere za ispravljanje faktora netačnosti podataka, ograniče rizike ili pogreške koje izrada profila može prouzrokovati i redovno ocjenjuju kvalitet podataka i algoritama koji se upotrebljavaju.

615 Modernizovana Konvencija br. 108, član 9. stav 1. tačka (a).

616 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 75.

617 Modernizovana Konvencija br. 108, član 9. stav 1. tačka (c).

618 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 77.

619 Savet Evrope, *Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling* (Preporuka CM/Rec(2010)13 Saveta ministara državama članicama o zaštiti pojedinaca u vezi s automatskom obradom ličnih podataka u kontekstu izrade profila), član 5. tačka (5).

6.2. Pravni lekovi, odgovornost, kazne i naknada

Ključne tačke

- U skladu sa modernizovanom Konvencijom br. 108, u domaćem zakonodavstvu ugovornih strana moraju da se propišu odgovarajući pravni lekovi i sankcije za kršenje prava na zaštitu podataka.
- OUZP-om se na nivou EU utvrđuju pravni lekovi za ispitanike u slučajevima povrede njihovih prava, kao i sankcije protiv rukovalaca podacima i obrađivača podataka koji se ne pridržavaju odredbi Uredbe. Njome se takođe utvrđuje pravo na naknadu štete i odgovornost.
  - Ispitanici imaju pravo na podnošenje prigovora nadzornom telu zbog navodnih kršenja Uredbe, kao i pravo na delotvoran pravni lek i dobijanje naknade štete.
  - Pri ostvarivanju prava na delotvoran pravni lek pojedince mogu zastupati neprofitne organizacije koje deluju u oblasti zaštite podataka.
  - Rukovalac podacima ili obrađivač podataka odgovoran je za svu materijalnu i nematerijalnu štetu koja nastane zbog kršenja prava.
  - Nadzorna tela imaju ovlašćenje izricanja upravnih novčanih kazni za kršenja Uredbe u iznosu do 20 000 000 EUR ili, u slučaju preduzeća, 4% od ukupnog godišnjeg prometa na svetskom nivou, u zavisnosti od toga šta je veće.
- Ispitanici mogu da podnesu prredstavke u vezi sa povredama prava zaštite podataka ESLJP-u, ali samo u krajnjoj nuždi i pod određenim uslovima.
- Svaka fizičko ili pravno lice ima pravo na podnošenje tužbe na bilo koju odluku Evropskog odbora za zaštitu podataka pred SPEU pod uslovima utvrđenima u Ugovorima.

Donošenje pravnih instrumenata nije dovoljno za obezbeđenje zaštite ličnih podataka u Evropi. Da bi evropski propisi o zaštiti podataka bili delotvorni, potrebno je uspostaviti mehanizme kojima se pojedincima omogućava da se suprotstave povredama svojih prava i da zatraže naknadu za bilo koju pretrpljenu štetu. Takođe je važno da nadzorna tela imaju pravo da izriču sankcije koje su delotvorne, odvraćajuće i srazmerne učinjenoj povredi [prava].

Prava koja štiti pravo zaštite podataka može da ostvari lice čija su prava dovedena u pitanje, odnosno ispitanik. Međutim, druga lica koja ispunjavaju odgovarajuće zahteve na osnovu domaćeg zakonodavstva takođe mogu zastupati ispitanike u postupku ostvarivanja njihovog prava. U skladu sa brojnim domaćim zakonima,

decu i osobe s intelektualnim teškoćama moraju zastupati njihovi staratelji[620]. Prema pravu zaštite podataka EU, udruženje čiji je zakonit cilj unapređenje prava na zaštitu podataka može zastupati ispitanike pred nadzornim telom ili sudom[621].

6.2.1. Pravo na podnošenje prigovora nadzornom telu

Prema pravu i **Saveta Evrope** i **Unije**, pojedinci imaju pravo da podnesu zahteve i prigovore nadležnom nadzornom telu ako smatraju da se obrada njihovih ličnih podataka ne vrši u skladu sa zakonom.

U modernizovanoj Konvenciji br. 108 potvrđuje se pravo ispitanika na pomoć nadzornog tela u ostvarivanju njihovih prava na osnovu Konvencije, nezavisno od njihovog državljanstvu ili prebivališta[622]. Zahtev za pomoć može se odbiti samo u izuzetnim okolnostima i ispitanici ne bi trebalo da snose troškove i naknade u vezi sa tom pomoći[623].

Slične odredbe se mogu pronaći i u pravnom sistemu EU. OUZP-om se propisuje da nadzorna tela donesu mere kojima će olakšati podnošenje prigovora, poput izrade obrasca za podnošenje prigovora elektronskim putem[624]. Ispitanik može podneti prigovor nadzornom telu u državi članici u kojoj ima uobičajeno boravište, u kojoj je njegovo radno mesto ili mesto navodnog kršenja[625]. Sadržaj prigovora se mora istražiti, a nadzorno telo mora obavestiti dotičnu osobu o ishodu postupka obrade prigivora[626].

Moguća kršenja propisa u institucijama i telima EU mogu se prijaviti Evropskom nadzorniku za zaštitu podataka (EDPS)[627]. Ako Evropski nadzornik za zaštitu podataka

620 FRA (2015.), *Priručnik o pravima deteta u evropskom pravu*, Luxembourg, Kancelarija za publikacije Evropske unije; FRA (2013.), *Legal capacity of persons with intellectual disabilities and persons with mental health problems* (Poslovna sposobnost osoba s intelektualnim teškoćama i osoba s mentalnim problemima), Luxembourg, Kancelarija za publikacije Evropske unije.

621 Opšta uredba o zaštiti podataka, član 80.

622 Modernizovana Konvencija br. 108, član 18.

623 *Ibid*., čl. 16 i 17.

624 Opšta uredba o zaštiti podataka, član 57. stav 2.

625 *Ibid*., član 77. stav 1.

626 *Ibid*., član 77. stav 2.

627 Uredba (EZ) br. 45/2001 Evropskog parlamenta i Saveta od 18. decembra 2000. o zaštiti pojedinaca u vezi s obradom ličnih podataka u institucijama i telima Zajednice i o slobodnom kretanju takvih podataka, SL 2001 L 8.

ne odgovori u roku od šest meseci, smatra se da je prigovor odbijen. Žalbe protiv odluka EDPS-a mogu se podneti SPEU u okviru Uredbe (EZ) br. 45/2001 kojom se institucijama i telima EU propisuje obaveza poštovanja pravila zaštite podataka.

Mora postojati mogućnost podnošenja obraćanja sudovima u vezi sa odlukama domaćeg nadzornog tela. To se odnosi na ispitanika, kao i na rukovaoce podacima koji su učestvovali u postupku pred nadzornim telom.

Primer: U septembru 2017. godine špansko nadležno telo za zaštitu podataka novčano je kaznilo Fejsbuk zbog kršenja nekoliko propisa o zaštiti podataka. Nadzorno telo osudilo je tu društvenu mrežu zbog prikupljanja, čuvanja i obrade ličnih podataka u oglašivačke svrhe, uključujući posebne kategorije ličnih podataka, bez dobijanja pristanka ispitanika. Odluka je donesena na osnovu istrage koju je nadzorno telo sprovelo na sopstvenu inicijativu.

6.2.2. Pravo na delotvoran pravni lek

Uz pravo na podnošenje prigovora nadzornom telu, pojedinci moraju imati pravo na delotovran pravni lek i pokretanje sudskog postupka. Pravo na pravni lek dobro je zaštićeno u evropskoj pravnoj tradiciji, tako da je prepoznato kao temeljno pravo i članom 47. Povelje EU o osnovnim pravima i članom 13. EKLJP-a[628].

Unutar prava EU, važnost stavljanja delotvornog pravnog leka na raspolaganje ispitanicima u slučaju povrede njihovih prava jasna je iz odredbi OUZP-a, kojima se utvrđuje pravo na delotovran pravni lek protiv nadzornih tela, rukovalaca podacima i obrađivača podataka, kao i iz sudske prakse Suda pravde EU.

Primer: U predmetu *Schrems*[629] SPEU je Odluku o primerenosti sigurne luke proglasio nevažećom. Tom odlukom su bili dopušteni međunarodni prenosi podataka iz EU organizacijama u SAD koje vrše sopstveno potvrđivanje u sklopu sistema sigurne luke. SPEU je smatrao da sistem sigurne luke ima nekoliko nedostataka zbog kojih se ugrožavaju osnovna prava građana EU na zaštitu privatnosti, zaštitu ličnih podataka i pravo na delotvoran pravni lek.

628 Videti na primer ESLJP, *Karabeyoğlu protiv Turske*, br. 30083/10, 7. juna 2016; ESLJP, *Mustafa Sezgin Tanrıkulu protiv Turske*, br. 27473/06, 18. jula 2017.

629 SPEU, C-362/14, *Maximillian Schrems protiv Data Protection Commissioner* [VV], 6. oktobra 2015.

U pogledu povrede prava na privatnost i zaštitu podataka, SPEU je istakao da se zakonima SAD određenim organima javne vlasti dopušta pristup ličnim podacima koji su preneseni iz država članica [EU] u SAD i njihova obrada na način koji nije u skladu sa svrhama zbog kojih su izvorno preneseni i koji prekoračuje ono što je strogo nužno i srazmerno nacionalnoj bezbednosti. U pogledu prava na delotvoran pravni lek, SPEU je napomenuo da ispitanici nemaju mogućnost pristupa i po potrebi ispravljanja ili brisanja podataka o sebi upravnim ili sudskim putem. SPEU je zaključio da propis koji ne pruža nikakvu mogućnost korišćenja pravnih sredstava radi pristupa ličnim podacima, ili radi ispravke ili brisanja takvih podataka, „ne poštuje bitan sadržaj osnovnog prava na delotvornu sudsku zaštitu, kao što je to propisano u članu 47. Povelje". Naglasio je da je postojanje pravnog leka kojim se obezbeđuje poštovanje pravnih odredbi svojstveno vladavini prava.

Pojedinci, rukovaoci podacima ili obrađivači podataka koji žele da ospore pravno obavezujuću odluku nadzornog tela mogu da pokrenu postupak pred sudom[630]. Pojam „odluka" treba da se tumači u širem smislu, tako da obuhvata izvršenje istražnih ovlašćenja, ovlašćenja sankcionisanja i odobravanja nadzornog tela, kao i odluke o odbacivanju ili odbijanju prigovora. Međutim, mere koje nisu pravno obavezujuće, poput mišljenja ili saveta koje je dalo nadzorno telo, ne mogu biti predmet sudskog postupka[631]. Postupci protiv nadzornog tela moraju se voditi pred sudovima države članice u kojoj ono ima sedište[632].

U slučajevima u kojima rukovalac podacima ili obrađivač podataka povredi prava ispitanika, ispitanik ima pravo da podnese tužbu sudu[633]. U postupcima pokrenutim protiv rukovaoca podacima ili obrađivača podataka posebno je važno da pojedinci imaju mogućnost izbora mesta pokretanja postupka. Mogu ih voditi u državi članici u kojoj rukovalac podacima ili obrađivač podataka ima sedište ili u državi članici u kojoj dotični ispitanik ima redovno boravište[634]. Druga mogućnost olakšava pojedincima da ostvare svoja prava jer im omogućava pokretanje postupka u državi u kojoj borave i u sudskoj nadležnosti koju poznaju. Ograničavanje mesta za pokretanje postupaka protiv rukovaoca podacima i obrađivača podataka na državu članicu u kojoj oni imaju sedište moglo bi da odvrati ispitanike da pokrenu sudske postupke

630 Opšta uredba o zaštiti podataka, član 78.

631 *Ibid*., uvodna izjava 143.

632 *Ibid*., član 78. stav 3.

633 *Ibid*., član 79.

634 *Ibid*., član 79. stav 2.

ako žive u drugim državama članicama, jer bi to uključivalo putovanje i dodatne troškove, dok bi sam postupak mogao da se vodi na stranom jeziku i u nepoznatoj nadležnosti. Jedini izuzetak su predmeti u kojima je rukovalac podacima ili obrađivač podataka javno telo, a postupak se vodi u sklopu izvršavanja njihovih javnih ovlašćenja. U tom slučaju su za predmet nadležni samo sudovi države u kojoj se nalazi dotično javno telo[635].

U većini slučajeva predmeti koji se odnose na propise o zaštiti podataka rešavaće se pred sudovima država članica, ali neki predmeti se mogu voditi i pred SPEU. Prva mogućnost se odnosi na slučaj u kojem ispitanik, rukovalac podacima, obrađivač podataka ili nadzorno telo pokreće postupak za poništenje odluke EOZP-a. Međutim, budući da takav postupak podleže uslovima iz člana 263. UFEU, da bi bio valjan, ti pojedinci i subjekti moraju da dokažu da se odluka Odbora neposredno i lično odnosi na njih.

Drugi scenario se odnosi na slučajeve u kojima institucije i tela EU nezakonito obrađuju lične podatke. U slučajevima u kojima institucije Evropske unije krše pravo zaštite podataka, ispitanici mogu da podnesu tužbu Opštem sudu Evropske unije (Opšti sud je deo SPEU). Opšti sud je odgovoran za donošenje prvostepenih odluka o tužbama povodom povreda prava Unije koje čine institucije EU. Zato se tužbe protiv EDPS-a, koji je institucija EU, takođe mogu podneti Opštem sudu[636].

Primer: U predmetu *Bavarian Lager*[637] ta kompanija je od Evropske komisije zatražila pristup celokupnom zapisniku sa sastanka koji je održala Komisija, a koji se navodno odnosio na pravna pitanja bitna za kompaniju. Komisija je odbila zahtev kompanije iz razloga prevladavajućih interesa zaštite podataka[638]. Pozivajući se na član 32. Uredbe o zaštiti podataka u institucijama Evropske unije, kompanija Bavarian Lager protiv te odluke je uložila žalbu Prvostepenom sudu (prethodniku Opšteg suda). U svojoj odluci (predmet T-194/04, *The Bavarian Lager Co. Ltd protiv Komisije Evropskih zajednica*) Prvostepeni sud je poništio odluku Komisije kojom je odbijen zahtev za pristup. Evropska komisija žalila se na tu odluku SPEU.

635 *Ibid.*

636 Uredba (EZ) br. 45/2001, član 32. stav 3.

637 SPEU, C-28/08 P, *Evropska komisija protiv The Bavarian Lager Co. Ltd* [VV], 2010.

638 Detaljna analiza rasprave dostupna je u publikaciji EDPS (2011), *Public access to documents containing personal data after the Bavarian Lager ruling* (Javni pristup dokumentima koji sadrže lične podatke nakon presude u predmetu Bavarian Lager), Bruxelles, EDPS.

Veliko Veće SPEU donelo je presudu kojom je odbačena presuda Prvostepenog suda i potvrđeno Komisijsko odbacivanje zahteva za pristup celokupnom zapisniku sa sastanka radi zaštite ličnih podataka osoba koje su prisustvovale sastanku. SPEU je smatrao da Komisija nije smela da otkrije te podatke budući da učesnici sastanka nisu dali pristanak za otkrivanje svojih ličnih podataka. Usto, kompanija Bavarian Lager nije dokazala da joj je nužan pristup tim informacijama.

Tokom odvijanja domaćeg postupka, ispitanici, nadzorna tela, rukovaoci podacima ili obrađivači podataka mogu od domaćeg suda da zatraže da zahteva objašnjenje od Suda EU o tumačenju i valjanosti akata institucija, tela, kancelarija ili agencija Evropske unije. Takva objašnjenja se nazivaju prethodnim odlukama. To nije neposredni lek za podnosioca, ali domaćim sudovima omogućava primenu tačnog tumačenja prava Unije. Upravo putem tog mehanizma prethodnih odluka ključni predmeti za razvoj prava zaštite podataka EU došli su do SPEU, na primer predmeti *Digital Rights Ireland* i *Kärntner Landesregierung i dr.*[639], kao i *Schrems*[640].

Primer: *Digital Rights Ireland* i *Kärntner Landesregierung i drugi*[641] spojeni je predmet koji su podneli irski Visoki sud (High Court) i austrijski Ustavni sud u vezi sa usklađenošću Direktive 2006/24/EZ (Direktive o zadržavanju podataka) sa pravom zaštite podataka EU. Austrijski Ustavni sud je SPEU podneo pitanja u vezi sa valjanošću članova od 3. do 9. Direktive 2006/24/EZ u svetlu članova 7., 9. i 11. Povelje EU o osnovnim pravima. Pitanja su se odnosila na to da li su određene odredbe austrijskog Saveznog zakona o telekomunikacijama, kojima se prenosi Direktiva o zadržavanju podataka, neusklađene s aspektima nekadašnje Direktive o zaštiti podataka i Uredbe o zaštiti podataka u institucijama Evropske unije.

U predmetu *Kärntner Landesregierung i dr.* g. Zajtlinger, jedan od tužilaca u postupku pred Ustavnim sudom, tvrdio je da telefon, internet i e-poštu upotrebljava i u poslovne i u privatne svrhe. U skladu s tim, informacije koje

639 SPEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr. i Kärntner Landesregierung i dr.* [VV], 8. aprila 2014.

640 SPEU, C-362/14, *Maximillian Schrems protiv Data Protection Commissioner* [VV], 6. oktobra 2015.

641 SPEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr. i Kärntner Landesregierung i dr.* [VV], 8. aprila 2014.

je slao i primao prolazile su kroz javne telekomunikacione mreže. Prema austrijskom Zakonu o telekomunikacijama iz 2003. godine, njegov pružalac telekomunikacionih usluga bio je zakonski obavezan da prikuplja i čuva podatke o njegovoj upotrebi mreže. G. Zajtlinger smatrao je da takvo prikupljanje i čuvanje njegovih ličnih podataka nije bilo nužno u tehničke svrhe slanja i primanja informacija putem mreže. Osim toga, prikupljanje i čuvanje tih podataka nisu nikako bili nužni u svrhu naplate. G. Zajtlinger izjavio je da nije pristao na takvu upotrebu svojih ličnih podataka, koji su prikupljeni i čuvani isključivo zbog austrijskog Zakona o telekomunikacijama iz 2003. godine.

Stoga je g. Zajtlinger pred austrijskim Ustavnim sudom pokrenuo postupak u kojem je tvrdio da se zakonskim obavezama njegovog pružaoca telekomunikacionih usluga krše njegova osnovna prava prema članu 8. Povelje EU o osnovnim pravima. Budući da je u austrijskom zakonodavstvu sprovedeno pravo Unije (tadašnja Direktiva o zadržavanju podataka), austrijski Ustavni sud je uputio predmet SPEU kako bi on doneo odluku o usklađenosti Direktive s pravima na privatnost i zaštitu podataka zaštićenima Poveljom EU o osnovnim pravima.

Veliko Veće SPEU donelo je odluku o predmetu, koja je dovela do poništavanja Direktive EU o zadržavanju podataka. SPEU je utvrdio da je Direktiva uključivala posebno ozbiljno mešanje u osnovna prava na privatnost i zaštitu podataka, koje nije bilo ograničeno na ono što je strogo nužno. Direktiva je imala legitiman cilj, jer su njome domaćim telima pružene dodatne mogućnosti za istragu i gonjenje teških krivičnih dela, pa je stoga bila koristan alat za krivične istrage. Međutim, SPEU je napomenuo da ograničenja osnovnih prava treba da se primenjuju samo ako su strogo nužna i da treba da budu propraćena jasnim i preciznim pravilima o njihovoj oblasti primene, zajedno sa zaštitnim merama za pojedince.

Prema mišljenju SPEU, Direktiva nije ispunjavala taj kriterijum nužnosti. Za početak, njome nisu utvrđena jasna i precizna pravila kojima se ograničava opseg mešanja. Umesto postavljanja zahteva za povezanost zadržanih podataka sa teškim krivičnim delima, Direktiva se primenjivala na sve metapodatke svih korisnika svih elektronskih komunikacionih sredstava. Stoga je predstavljala mešanje u prava na privatnost i zaštitu podataka gotovo cele populacije EU, što se može smatrati nesrazmernim. Nije sadržala uslove za ograničenje broja osoba koje su ovlašćene za pristup ličnim podacima, niti je takav pristup podlegao procesnim uslovima kao što je zahtev za odobrenje upravnog tela ili suda pre samog pristupa. Konačno, Direktivom nisu utvrđene jasne zaštitne

mere za zaštitu zadržanih podataka. Stoga, njome nije omogućena efikasna zaštita podataka od rizika zloupotrebe, kao i od svih nezakonitih pristupa ili korišćenja tih podataka[642].

SPEU u načelu mora da odgovori na postavljena prethodna pitanja i ne može odbiti donošenje odluke po istima po osnovu toga što smatra da nisu relevantna za izvorni predmet, ili nisu postavljena na vreme.. Međutim, može odbiti donošenje odluke ako pitanje nije unutar njegove nadležnosti[643]. SPEU donosi odluku samo o sastavnim delovima upućenog prethodnog pitanja, a domaći sud zadržava nadležnost u odlučivanju u izvornom predmetu[644].

Prema pravu Saveta Evrope ugovorne strane moraju uspostaviti odgovarajuće sudske i nesudske pravne lekove za povrede odredbi modernizovane Konvencije br. 108[645]. Predstavke povodom navodnih povreda prava na zaštitu podataka iz člana 8. EKLJP-a koje učini ugovorna strana EKLJP-a mogu se dodatno podneti Evropskom sudu za ljudska prava nakon što se iscrpu svi dostupni domaći pravni lekovi. Da bi predstavka zbog povreda člana 8. EKLJP-a bila podneta ESLJP-u treba da budu ispunjeni i drugi uslovi prihvatljivosti (članovi 34. i 35. EKLJP-a)[646].

Iako zahtevi ESLJP-u mogu biti usmereni samo protiv ugovornih strana, posredno se mogu baviti i postupcima ili propustima privatnih strana, pod uslovom da ugovorna strana nije ispunila svoje pozitivne obaveze prema EKLJP-u, niti je obezbedila dovoljnu zaštitu protiv povrede prava na zaštitu podataka u svom domaćem zakonodavstvu.

Primer: U predmetu *K. U. protiv Finske*,[647] podnosilac predstavke, maloletnik, žalio se da je o njemu objavljen oglas seksualne prirode na internet stranici za upoznavanje. Pružalac usluge nije otkrio identitet osobe koja je objavila

642 SPEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr. i Kärntner Landesregierung i dr.* [VV], 8. aprila 2014, stav 69.

643 SPEU, C-244/80, *Pasquale Foglia protiv Mariella Novello* (br. 2), 16. decembra 1981.; SEU, C-467/04, *Krivični postupak protiv Giuseppe Francesco Gasparini i dr.*, 28. septembra 2006.

644 SPEU, C-438/05, *International Transport Workers' Federation i Finnish Seamen's Union protiv Viking Line ABP i OÜ Viking Line Eesti* [VV], 11. decembra 2007, stav 85.

645 Modernizovana Konvencija br. 108, član 12.

646 EKLJP, članovi od 34 do 37.

647 ESLJP, *K. U. protiv Finske*, br. 2872/02, 2. decembra 2008.

informacije zbog obaveza poverljivosti prema finskom zakonodavstvu. Podnosilac predstavke je tvrdio da finskim zakonodavstvom nije obezbeđena dovoljna zaštita od takvih radnji privatne osobe koja je na internetu objavila inkriminišuće podatke o njemu. ESLJP je smatrao da su države dužne da se uzdrže se od proizvoljnog mešanja u privatne živote pojedinaca i da mogu podlegati pozitivnim obavezama koje uključuju „donošenje mera za obezbeđivanje poštovanja privatnog života, čak i u okviru međusobnih odnosa pojedinaca". U slučaju podnosioca predstavke njegova praktična i delotvorna zaštita zahtevala je preduzimanje konkretnih koraka za identifikaciju i gonjenje učinitelja. Međutim, država nije obezbedila takvu zaštitu, stoga je ESLJP zaključio da je došlo do povrede člana 8. Konvencije.

Primer: U predmetu *Köpke protiv Nemačke*[648] podnositeljka predstavke je osumnjičena za krađu na radnom mestu, pa je podvrgnuta tajnom video-nadzoru. ESLJP je zaključio da „ništa ne upućuje na to da domaća nadležna tela nisu uspostavila poštenu ravnotežu, u okviru svog polja slobodne procene, između prava podnositejke predstavke na poštovanje njenog privatnog života prema članu 8. i interesa njenog poslodavca da zaštiti svoja vlasnička prava i javnog interesa za ispravnom primenom pravde". Zato je predstavka proglašena neprihvatljivom.

Ako ESLJP utvrdi da je država koja je ugovorna strana povredila bilo koja prava koja se štite Evropskom konvencijom o ljudskim pravima, ta ugovorna strana mora da izvrši presudu ESLJP-a (član 46. Konvencije). Izvršnim merama treba prvo zaustaviti povredu i ispraviti, koliko je to moguće, negativne posledice povreda po podnosioca predstavke. Izvršenje presuda može iziskivati i opšte mere kojima se sprečavaju povrede slične onima koje je utvrdio ESLJP, bilo unosom promena u zakonodavstvo, sudsku praksu ili na drugi način.

Ako ESLJP utvrdi povredu Evropske konvencije o ljudskim pravima, njenim članom 41. propisano je da taj sud može tužiocu dosuditi „pravično zadovoljenje" o trošku ugovorne strane.

Pravo na ovlašćenje neprofitnog tela, organizacije ili udruženja

OUZP-om se pojedincima koji podnose tužbu nadzornom telu ili pokreću sudski postupak omogućava da ovlaste neprofitno telo, organizaciju ili udruženje da ih

648 ESLJP, *Köpke protiv Nemačke* (odl.), br. 420/07, 5. oktobra 2010.

zastupa[649]. Ta neprofitna tela moraju imati ciljeve od javnog interesa u svom statutu i biti aktivna u oblasti zaštite podataka. Ona mogu da podnose prigovore ili zastupaju ispitanike pred sudskim organima. Uredbom se državama članicama pruža mogućnost da, u skladu sa svojim domaćim zakonodavstvom, odluče da li takvo telo može da podnosi tužbe u ime ispitanika bez njihovog posebnog ovlašćenja za to.

To pravo zastupanja omogućava pojedincima da iskoriste stručna znanja i organizacione i finansijske resurse takvih neprofitnih tela i tako lakše ostvare svoja prava. OUZP-om se omogućava da takva tela podnose kolektivne zahteve u ime više ispitanika. Time se doprinosi funkcionisanju i delotvornosti pravosudnog sistema, jer se slični zahtevi grupišu i zajednički razmatraju.

6.2.3. Odgovornost i pravo na naknadu štete

Pravom na delotvoran pravni lek pojedincima se mora pružiti mogućnost da zatraže naknadu za bilo kakvu štetu koju pretrpe zbog obrade njihovih ličnih podataka na način kojim se krši merodavno zakonodavstvo. Odgovornost rukovaoca podacima i obrađivača podataka za nezakonitu obradu izričito se spominje u OUZP-u[650]. Uredbom se pojedincima dodeljuje pravo na naknadu štete od rukovaoca podacima ili obrađivača podataka za materijalnu i nematerijalnu štetu, dok se u uvodnim izjavama utvrđuje sledeće: „pojam štete trebalo bi široko tumačiti s obzirom na sudsku praksu Suda tako da se u potpunosti odražavaju ciljevi ove Uredbe"[651]. Rukovaoci podacima snose odgovornost i mogu biti izloženi zahtevima za naknadu štete ako ne ispunjavaju svoje obaveze na osnovu Uredbe. Obrađivači ličnih podataka odgovorni su za štetu prouzrokovanu obradom samo kada ona nije bila u skladu s obavezama iz Uredbe koje se izričito odnose na obrađivača podataka ili kada je izvršena mimo zakonitih uputstava rukovalaca podacima ili suprotno njima. Ako je rukovalac podacima ili obrađivač podataka platio punu odštetu, OUZP-om se utvrđuje da taj rukovalac podacima ili obrađivač podataka može da zatraži od drugih rukovalaca podacima ili obrađivača podataka, koji su uključeni u istu obradu, da plate deo odštete koji odgovara njihovom udelu u odgovornosti za štetu[652]. Izuzeća od odgovornosti vrlo su stroga i zahtevaju dokaz da rukovalac podacima ili obrađivač podataka ni na koji način nije odgovoran za događaj koji je prouzrokovao štetu.

649 Opšta uredba o zaštiti podataka, član 80.

650 *Ibid*., član 82.

651 *Ibid*., uvodna izjava 146.

652 *Ibid*., član 82. st. 2 i 5.

Naknada mora biti „potpuna i stvarna" s obzirom na pretrpljenu štetu. Ako je šteta prouzrokovana obradom nekoliko rukovalaca podacima ili obrađivača podataka, svaki rukovalac podacima ili obrađivač podataka mora snositi odgovornost za svu štetu. Tim pravilom se nastoji da se obezbedi stvarna naknada za ispitanike i koordinisani pristup usklađenosti rukovalaca podacima i obrađivača podataka koji učestvuju u aktivnostima obrade.

Primer: Ispitanici ne moraju da pokrenu postupak i zatraže naknadu štete od svih tela odgovornih za štetu jer to može podrazumevati visoke troškove i dugotrajne postupke. Dovoljno je pokrenuti postupak protiv jednog od zajedničkih rukovalaca podacima koji će snositi odgovornost za svu štetu. U takvim slučajevima rukovalac podacima ili obrađivač podataka koji plati odštetu naknadno ima pravo na povrat dela plaćenog iznosa od drugih tela uključenih u obradu i odgovornih za povredu srazmerno njihovom delu odgovornosti za štetu. Ti postupci između različitih zajedničkih rukovalaca podacima i obrađivača podataka odvijaju se nakon što ispitanik primi naknadu i on u njima ne učestvuje.

Unutar pravnog okvira Saveta Evrope, članom 12. modernizovane Konvencije br. 108 propisuje se obaveza za ugovorne strane da uvedu odgovarajuće pravne lekove za povrede domaćeg prava kojim se izvršavaju odredbe Konvencije. U Izveštaju s objašnjenjima o modernizovanoj Konvenciji br. 108 navodi se da pravni lekovi moraju uključivati mogućnost sudskog preispitivanja odluke ili prakse i da moraju biti dostupni i vansudski pravni lekovi[653]. Odluke o pojedinim modalitetima i pravilima povezanim sa pristupom tim pravnim lekovima, kao i postupci koje treba slediti, prepušteni su svakoj ugovornoj strani. Ugovorne strane i domaći sudovi treba da razmotre i uvođenje odredbi o novčanoj naknadi za materijalnu i nematerijalnu štetu prouzrokovanu obradom, kao i mogućnost pokretanja kolektivnih postupaka[654].

6.2.4. Sankcije

Unutar prava Saveta Evrope, članom 12. modernizovane Konvencije br. 108 propisano je da svaka ugovorna strana mora uspostaviti odgovarajuće sankcije i pravne lekove za kršenja odredbi domaćeg zakonodavstva kojima se sprovode osnovna načela zaštite podataka utvrđena u Konvenciji br. 108. Konvencijom se ne uspostavljaju niti nameću određene sankcije. Upravo suprotno, u njoj se jasno ističe da

653 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 100.

654 *Ibid*.

svaka ugovorna strana prema sopstvenom nahođenju može da odredi prirodu sudskih i vansudskih sankcija, koje mogu biti krivične, upravne ili građanskopravne. U Izveštaju s objašnjenjima o modernizovanoj Konvenciji br. 108 navodi se da sankcije moraju biti delotvorne, srazmerne i odvraćajuće[655]. Ugovorne strane moraju da se pridržavaju tog načela pri određivanju prirode i težine sankcija koje su dostupne na osnovu njihovog domaćeg pravnog poretka.

Unutar prava EU, članom 83 OUZP-a nadzorna tela država članica ovlašćuju se za izricanje upravnih novčanih kazni za kršenja Uredbe. Iznos novčanih kazni, okolnosti koje domaća tela moraju uzeti u obzir pri odlučivanju o izricanju kazne, kao i ukupne gornje granice iznosa novčanih kazni, takođe su propisani članom 83. Tako je sistem izricanja sankcija usklađen u celoj EU.

U OUZP-u se primenjuje pristup novčanim kaznama zasnovan na više nivoa. Nadzorna tela imaju ovlašćenje izricanja upravnih novčanih kazni za kršenja Uredbe u iznosu do 20 000 000 EUR ili, u slučaju preduzeća, 4 % od ukupnog godišnjeg prometa na svetskom nivou, u zavisnosti od toga šta je veće. Kršenja za koja se može izreći taj nivo novčane kazne uključuju povrede osnovnih načela za obradu i uslova pristanka, povrede prava ispitanika i odredbi Uredbe kojima se uređuje prenos ličnih podataka primaocima u trećim zemljama. Za druga kršenja nadzorna tela mogu izreći novčane kazne u iznosu do 10 000 000 EUR ili, u slučaju preduzeća, 2 % od ukupnog godišnjeg prometa na svetskom nivou, u zavisnosti od toga šta je veće.

Pri određivanju vrste i nivoa novčane kazne koja se izriče, nadzorna tela moraju uzeti u obzir niz činilaca[656]. Na primer, moraju posvetiti pažnju prirodi, ozbiljnosti i trajanju kršenja, kategorijama zahvaćenih ličnih podataka, kao i da li kršenje ima obeležje namere ili nepažnje. U obzir takođe treba uzeti svaku radnju koju je rukovalac podacima ili obrađivač podataka preduzeo kako bi ublažio štetu koju su pretrpeli ispitanici. Drugi važni činioci koji nadzornim telima pomažu u donošenju odluke su stepen saradnje sa nadzornim telom posle kršenja, način na koji je nadzorno telo saznalo za kršenje (na primer, da li je o njemu izvestilo telo nadležno za obradu ili ispitanik čija su prava povređena)[657].

655 *Ibid.*

656 Opšta uredba o zaštiti podataka, član 83. stav 2.

657 Radna grupa iz člana 29. (2017), *Smernice o primeni i određivanju upravnih novčanih kazni za potrebe Uredbe 2016/679,* WP 253, 3. oktobra 2017.

Uz mogućnost izricanja upravnih novčanih kazni, nadzorna tela na raspolaganju imaju širok niz drugih korektivnih mera. Takozvana „korektivna" ovlašćenja nadzornih tela utvrđena su članom 58. OUZP-a. Ona uključuju izdavanje naredbi, upozorenja i službenih opomena rukovaocima podacima i obrađivačima podataka i privremenu ili čak trajnu zabranu aktivnosti obrade.

U pogledu sankcija protiv povreda prava Unije koja učine institucije ili tela EU, zbog posebnog ovlašćenja Uredbe o zaštiti podataka u institucijama Evropske unije, sankcije mogu biti predviđene samo u obliku disciplinskih mera. Prema članu 49. te Uredbe, „[s]vaki propust u poštovanju obaveza prema ovoj Uredbi, bilo da je nameran ili posledica nemara funkcionera ili nekog drugog službenika Evropskih zajednica, čini ih podložnim disciplinskom postupku [...]".

7

Međunarodni prenos podataka i protok ličnih podataka

EU	Obuhvaćena pitanja	Savet Evrope
Prenosi ličnih podataka		
Opšta uredba o zaštiti podataka, član 44.	Koncept	Modernizovana Konvencija br. 108, član 14. stavovi 1. i 2.
Slobodan protok ličnih podataka		
Opšta uredba o zaštiti podataka, član 1. stav 3. i uvodna izjava 170	Među državama članicama Evropske unije	
	Među ugovornim stranama Konvencije br. 108	Modernizovana Konvencija br. 108, član 14. stav 1.
Prenosi ličnih podataka trećim zemljama ili međunarodnim organizacijama		
Opšta uredba o zaštiti podataka, član 45. C-362/14, *Maximillian Schrems protiv Data Protection Commissioner* [VV], 2015.	Odluka o primerenosti / treće zemlje ili međunarodne organizacije s odgovarajućim nivoima zaštite	Modernizovana Konvencija br. 108, član 14. stav 2.
Opšta uredba o zaštiti podataka, član 46. stav 1. i član 46. stav 2.	Odgovarajuće zaštitne mere, uključujući izvršna prava i pravne lekove za ispitanike, koje se daju putem standardnih ugovornih klauzula, obavezujućih korporativnih pravila, kodeksa ponašanja i mehanizama sertifikovanja	Modernizovana Konvencija br. 108, član 14. stavovi 2., 3., 5. i 6.

EU	Obuhvaćena pitanja	Savet Evrope
Opšta uredba o zaštiti podataka, član 46. stav 3.	Uslovljeno odobrenjem nadležnog nadzornog tela: ugovorne klauzule i odredbe sadržane u administrativnim dogovorima između javnih tela	
Opšta uredba o zaštiti podataka, član 46. stav 5.	Postojeća odobrenja na osnovu Direktive 95/46/EZ	
Opšta uredba o zaštiti podataka, član 47.	Obavezujuća korporativna pravila	
Opšta uredba o zaštiti podataka, član 49.	Odstupanja za posebne situacije	Modernizovana Konvencija br. 108, član 14. stav 4.
Primeri: Sporazum između EU i SAD o podacima iz evidencije podataka o putnicima Sporazum SWIFT između EU i SAD	Međunarodni sporazumi	Modernizovana Konvencija br. 108, član 14. stav 3. tačka (a)

U okviru prava Unije, Opštom uredbom o zaštiti podataka uređuje se slobodan protok podataka unutar Evropske unije. Međutim, ona sadrži posebne zahteve koji se odnose na prenose ličnih podataka trećim zemljama izvan EU i međunarodnim organizacijama. Uredbom se potvrđuje važnost takvih prenosa, posebno u kontekstu međunarodne trgovine i saradnje, ali prepoznaje se i povećan rizik za lične podatke. Uredbom se stoga nastoji da se pruži nivo zaštite za prenos ličnih podataka u treće zemlje koji je jednak onoj unutar EU[658]. Pravom Saveta Evrope takođe se potvrđuje važnost primene pravila za prekogranične prenose podataka na osnovu slobodnog protoka među stranama i posebnih zahteva za prenose drugim stranama.

7.1. Priroda prenosa ličnih podataka

Ključne tačke

- Evropska unija i Savet Evrope imaju propise o prenosima ličnih podataka primaocima u trećim zemljama ili međunarodnim organizacijama.
- Obezbeđenjem zaštite prava ispitanika prilikom prenosa podataka izvan EU omogućava se zadržavanje zaštite propisane pravom EU za lične podatke poreklom iz EU.

658 Opšta uredba o zaštiti podataka, uvodne izjave 101 i 116.

Prema **pravu Saveta Evrope**, prekogranični prenosi podataka opisuju se kao prenosi ličnih podataka primaocima koji podležu nadležnosti drugih država[659]. Prekogranični prenosi podataka primaocu koji ne podleže nadležnosti ugovorne strane dozvoljeni su samo ako je prisutan odgovarajući nivo zaštite[660].

Pravom EU uređuju se prenosi „ličnih podataka koji se obrađuju ili su namenjeni obradi posle prenosa u treću zemlju ili međunarodnu organizaciju [...]"[661]. Takvi prenosi podataka su dozvoljeni samo ako su usklađeni sa pravilima iz poglavlja V OUZP-a.

Prekogranični prenosi ličnih podataka dopušteni su prema primaocima koji podležu nadležnosti ugovorne strane Saveta Evrope ili države članice EU. U oba pravna sistema dozvoljava se prenos podataka u zemlju koja nije ugovorna strana niti država članica ako su ispunjeni određeni uslovi.

7.2. Slobodno kretanje/protok ličnih podataka među državama članicama ili ugovornim stranama

Ključne tačke

- Protok ličnih podataka kroz EU i prenosi ličnih podataka među ugovornim stranama modernizovane Konvencije br. 108 ne smeju da budu ograničeni. Međutim, budući da nisu sve ugovorne strane modernizovane Konvencije br. 108 države članice EU, prenosi iz države članice EU u treću zemlju koja jeste ugovorna strana modernizovane Konvencije br. 108 nisu mogući ako ne ispunjavaju uslove utvrđene OUZP-om.

Prema pravu Saveta Evrope, mora se obezbediti slobodan protok ličnih podataka među ugovornim stranama modernizovane Konvencije br. 108. Međutim, prenos može biti zabranjen ako postoji „stvaran i ozbiljan rizik da bi prenos drugoj strani doveo do zaobilaženja odredbi Konvencije" ili ako je strana obavezna da to učini u skladu sa „usklađenim pravilima zaštite među državama koje pripadaju regionalnoj međunarodnoj organizaciji"[662].

659 Izveštaj s objašnjenjima o modernizovanoj Konvenciji br. 108, stav 102.

660 Modernizovana Konvencija br. 108, član 14. stav 2.

661 Opšta uredba o zaštiti podataka, član 44.

662 Modernizovana Konvencija br. 108, član 14. stav 1.

Unutar prava EU, slobodno kretanje ličnih podataka među državama članicama EU ne ograničava se niti zabranjuje iz razloga povezanih sa zaštitom pojedinaca u pogledu obrade ličnih podataka[663]. Oblast slobodnog prenosa podataka je proširena Sporazumom o evropskom ekonomskom prostoru (EGP)[664], kojim se Island, Lihtenštajn i Norveška uvode na unutrašnje tržište.

Primer: Ako podružnica međunarodne grupacije sa sedištem u nekoliko država članica, između ostalog u Sloveniji i Francuskoj, pošalje lične podatke iz Slovenije u Francusku, takav prenos podataka se ne sme ograničiti niti zabraniti slovenačkim domaćim zakonodavstvom iz razloga povezanih sa zaštitom ličnih podataka.

Međutim, ako ista slovenačka podružnica želi da prenese te lične podatke matičnoj kompaniji u Maleziji, slovenački izvoznik podataka mora uzeti u obzir pravila iz poglavlja V OUZP-a. Tim odredbama nastoje da se zaštite lični podaci ispitanika koji podležu nadležnosti EU.

Prema pravu Unije, prenosi ličnih podataka u države članice EGP-a u svrhe povezane sa sprečavanjem, istragom, otkrivanjem ili gonjenjem krivičnih dela ili izvršavanjem krivičnih sankcija podležu Direktivi 2016/680[665]. Time se takođe obezbeđuje da razmena ličnih podataka među nadležnim telima unutar Unije ne bude ograničena niti zabranjena iz razloga zaštite podataka. Prema pravu Saveta Evrope, obrada svih ličnih podataka (uključujući prekogranični prenos drugim ugovornicama Konvencije br. 108), bez izuzetaka na osnovu svrha ili područja delovanja, obuhvaćena je oblašću primene Konvencije br. 108, iako ugovorne strane mogu uvesti izuzetke. Svi članovi EGP-a takođe su ugovornice Konvencije br. 108.

663 Opšta uredba o zaštiti podataka, član 1. stav 3.

664 Odluka Saveta i Komisije od 13. decembra 1993. o sklapanju Sporazuma o Evropskom ekonomskom prostoru između Evropskih zajednica, njihovih država članica i Republike Austrije, Republike Finske, Republike Islanda, Kneževine Lihtenštajn, Kraljevine Norveške, Kraljevine Švedske i Švajcarske Konfederacije, SL 1994 L 1.

665 Direktiva (EU) 2016/680 Evropskog parlamenta i Saveta od 27. aprila 2016. o zaštiti pojedinaca u vezi s obradom ličnih podataka od strane nadležnih tela u svrhe sprečavanja, istrage, otkrivanja ili gonjenja krivičnih dela ili izvršavanja krivičnih sankcija i o slobodnom kretanju takvih podataka kao i o stavljanju izvan snage Okvirne odluke Saveta 2008/977/PUP, SL 2016 L119.

7.3. Prenosi ličnih podataka trećim zemljama / zemljama koje nisu strane ili međunarodnim organizacijama

Ključne tačke

- I **Savet Evrope** i **EU** dopuštaju prenose ličnih podataka trećim zemljama ili međunarodnim organizacijama ako su ispunjeni određeni uslovi za zaštitu ličnih podataka.
  - **Prema pravu Saveta Evrope**, odgovarajući nivo zaštite može se postići zakonodavstvom države ili međunarodne organizacije ili uspostavljanjem odgovarajućih standarda.
  - **Prema pravu EU**, prenosi se mogu odvijati ako treća zemlja obezbedi odgovarajuću nivo zaštite ili ako rukovalac podacima ili obrađivač podataka pruži odgovarajuće zaštitne mere, uključujući izvršna prava i pravne lekove za ispitanika, u obliku standardnih ugovornih klauzula ili obavezujućih korporativnih pravila.
- **I jednim i drugim pravom** predviđene su klauzule o odstupanju kojima se omogućava prenos ličnih podataka u posebnim okolnostima, čak i kada ne postoje odgovarajući nivo zaštite niti odgovarajuće zaštitne mere.

Iako se i pravom Saveta Evrope i pravom EU dopuštaju prenosi podataka trećim zemljama ili međunarodnim organizacijama, utvrđuju se različiti uslovi. U svakom skupu uslova se uzimaju u obzir različite strukture i svrhe pojedinih organizacija.

U sklopu **prava EU** u načelu postoje dva načina na koja je moguć prenos ličnih podataka u treće zemlje ili međunarodne organizacije. Prenosi ličnih podataka mogu se obavljati na osnovu odluke o primerenosti Evropske komisije[666] ili, u nedostatku takve odluke, kada rukovalac podacima ili obrađivač podataka pruži odgovarajuće zaštitne mere, uključujući izvršna prava i pravne lekove za ispitanika[667]. U nedostatku odluke o primerenosti ili odgovarajućih zaštitnih mera, moguća su brojna odstupanja.

666 Opšta uredba o zaštiti podataka, član 45.

667 *Ibid.*, član 46.

Međutim, u skladu sa pravom **Saveta Evrope**, slobodni prenosi podataka državama koje nisu ugovornice Konvencije dopušteni su samo na osnovu:

- zakona te države ili međunarodne organizacije, uključujući primenjive međunarodne ugovore ili sporazume kojima se garantuju odgovarajuće zaštitne mere,

- *ad hoc* ili odobrenih standardizovanih zaštitnih mera utvrđenih pravno obavezujućim i izvršnim instrumentima koje donose i vrše osobe uključene u prenos i dalju obradu[668].

Slično kao i unutar prava EU, u nedostatku odgovarajućeg nivoa zaštite podataka, dostupna su brojna odstupanja.

7.3.1. Prenosi na osnovu odluke o primerenosti

Unutar prava EU slobodan prenos podataka trećim zemljama s odgovarajućim nivoom zaštite podataka predviđen je članom 45. OUZP-a. SPEU je pojasnio da pojam „odgovarajući nivo zaštite" podrazumeva da treća zemlja osigurava nivo zaštite osnovnih prava i sloboda koji je „u načelu istovetan"[669] garancijama obezbeđenim pravom Unije. Istovremeno, sredstva koja koristi treća zemlja za obezbeđenje takvog nivoa zaštite mogu se razlikovati od onih koja se koriste u EU jer se standardom primerenosti ne zahteva potpuno preslikavanje propisa EU[670].

Evropska komisija procenjuje nivo zaštite podataka u drugim zemljama razmatranjem njihovog domaćeg zakonodavstva i primenjivih međunarodnih obaveza. U obzir uzima i učestvovanje pojedine države u multilateralnim ili regionalnim sistemima, naročito u vezi sa zaštitom ličnih podataka. Ako Evropska komisija zaključi da treća zemlja ili međunarodna organizacija obezbeđuje odgovarajuću nivo zaštite, može izdati odluku o primerenosti koja ima obavezujući efekat[671]. Međutim, SPEU je utvrdio da su domaća nadzorna tela ipak nadležna za ispitivanje zahteva određene osobe u vezi sa zaštitom njenih ličnih podataka koji su preneseni u treću zemlju za koju je Komisija utvrdila da obezbeđuje odgovarajuću nivo zaštite, nadovezujući

668 Modernizovana Konvencija br. 108, član 14. stav 3. tačke (a) i (b).

669 SPEU, C-362/14, *Maximillian Schrems protiv Data Protection Commissioner* [VV], 6. oktobra 2015, stav 96.

670 *Ibid*., stav 74. Videti i Evropska komisija (2017.), Komunikacija Komisije Evropskom parlamentu i Savetu „Razmena i zaštita ličnih podataka u globalizovanom svetu", COM(2017) 7 final od 10. januara 2017, str. 6.

671 Popis zemalja za koje je donesena odluka o primerenosti, koji se redovno ažurira, potražite na početnoj strani Evropske komisije, Glavne uprave za pravosuđe.

se na navode te osobe da važeće pravo i praksa u toj trećoj zemlji ne obezbeđuju odgovarajuću nivo zaštite[672].

Evropska komisija takođe može da proceni primerenost državnog područja u trećoj zemlji ili se ograniči na pojedine sektore, kao što je bio slučaj sa kanadskim zakonodavstvom o privatnoj komercijalnoj delatnosti[673]. Odluke o primerenosti za prenose mogu se donositi i na osnovu sporazuma između EU i trećih zemalja. Te odluke se odnose isključivo na jednu vrstu prenosa podataka, kao što su evidencije podataka o putnicima koje avio-kompanije prenose stranim telima za graničnu kontrolu kada avion leti iz Evropske unije u određena prekomorska odredišta (videti deo 7.3.4).

Odluke o primerenosti podležu stalnom nadzoru. Evropska komisija redovno preispituje takve odluke kako bi pratila razvoj događaja koji bi mogli da utiču na njihov status. Zato ako Evropska komisija utvrdi da treća zemlja ili međunarodna organizacija više ne ispunjava uslove iz odluke o primerenosti, odluku može izmeniti, obustaviti ili staviti van snage. Komisija takođe može pokrenuti pregovore sa predmetnom trećom zemljom ili međunarodnom organizacijom kako bi rešila problem iz odluke.

Odluke o primerenosti koje Evropska komisija donese na osnovu Direktive 95/46/EZ ostaju na snazi dok se ne izmene, zamene ili stave van snage odlukom Komisije donesenom u skladu sa pravilima iz člana 45. OUZP-a.

Do sada je Evropska komisija donela odluku da primerenu zaštitu pružaju Andora, Argentina, Kanada (komercijalne organizacije koje su obuhvaćene oblašću primene kanadskog Zakona o zaštiti ličnih podataka i o elektronskim dokumentima, odnosno *Personal Information and Electronic Documents Act* – PIPEDA), Farska ostrva, Grnzi, Ostrvo Man, Izrael, Džersi, Novi Zeland, Švajcarska i Urugvaj. U pogledu prenosa podataka u SAD, Evropska komisija donela je odluku o primerenosti 2000. godine, kojom su omogućeni prenosi kompanijama koje same potvrđuju da će štititi lične podatke prenesene iz EU i pridržavati se tzv. „načela sigurne luke"[674]. SPEU je poni-

672 SPEU, C-362/14, *Maximillian Schrems protiv Data Protection Commissioner* [VV], 6. oktobra 2015, st. 63, 65 i 66.

673 Evropska Komisija (2002.), Odluka 2002/2/EZ od 20. decembra 2001. u skladu s Direktivom 95/46/EZ Evropskog parlamenta i Saveta o odgovarajućoj zaštiti ličnih podataka propisanoj u Zakonu o zaštiti ličnih podataka i elektronskih dokumenata Kanade, SL 2002 L 2.

674 Odluka Komisije 2000/520/EZ od 26. jula 2000. u skladu sa Direktivom 95/46/EZ Evropskog parlamenta i Saveta o primerenosti zaštite koju pružaju načela privatnosti „sigurne luke" i uz njih vezana često postavljana pitanja koje je izdalo Ministarstvo trgovine SAD, SL L 215. SEU je Odluku proglasio nevažećom u predmetu C-632/14, *Maximillian Schrems protiv Data Protection Commissioner* [VV].

štio tu odluku 2015. pa je u julu 2016. godine donesena nova odluka o primerenosti kojom je kompanijama dozvoljeno da se pridruže od 1. avgusta 2016.

Primer: U predmetu *Schrems*[675] austrijski državljanin Maksimilijan Šrems bio je višegodišnji korisnik društvene mreže Fejsbuk. Neki ili svi podaci koje je g. Šrems dao Fejsbuku preneseni su iz irske podružnice Fejsbuka na servere u SAD, gde su oni i obrađeni. G. Šrems podneo je prigovor irskom nadležnom telu za zaštitu podataka, smatrajući da, s obzirom na otkrića američkog uzbunjivača Edvarda Snoudena o aktivnostima nadzora obaveštajnih službi SAD, zakoni i praksa SAD ne pružaju dovoljnu zaštitu za podatke prenesene u tu zemlju. Irsko telo je odbacilo prigovor pozivajući se na činjenicu da je Komisija u svojoj Odluci od 26. jula 2000. utvrdila da SAD obezbeđuje odgovarajuću nivo zaštite prenesenih ličnih podataka u sklopu sistema „sigurne luke". Predmet je iznesen pred irski Visoki sud, koji je uputio SPEU prethodno pitanje.

SPEU je presudio da je odluka Komisije o primerenosti okvira „sigurne luke" nevažeća. Prvo je istakao da je odlukom dozvoljeno ograničenje primenjivosti načela „sigurne luke" za zaštitu podataka na osnovu nacionalne bezbednosti, javnog interesa ili uslova za sprovođenje zakona ili na osnovu nacionalnog zakonodavstva u SAD. Odlukom je zato omogućeno mešanje u osnovna prava osoba čiji su lični podaci preneseni ili bi mogli biti preneseni u SAD[676]. Zatim je napomenuo da odluka ne sadrži nikakvo utvrđenje o postojanju pravila SAD za ograničavanje takvog mešanja u osnovna prava niti o bilo kakvoj delotvornoj pravnoj zaštiti protiv mešanja takve prirode[677]. SPEU je naglasio da nivo zaštite osnovnih prava i sloboda garantovanih u Evropskoj uniji zahteva da se u propisima kojima se zadire u osnovna prava garantovana u članovima 7. i 8. predvide jasna i precizna pravila koja uređuju opseg i primenu mere i propišu minimalne zaštitne mere, odstupanja i ograničenja u zaštiti ličnih podataka[678]. Budući da u Odluci Komisije nije utvrđeno da SAD zaista obezbeđuje odgovarajuću nivo zaštite na osnovu svog domaćeg zakonodavstva ili preuzetih međunarodnih obaveza, SPEU je zaključio da ne ispunjava zahteve relevantne odredbe o prenosu iz Direktive o zaštiti podataka i da stoga nije važeća[679].

675 SPEU, C-362/14, *Maximillian Schrems protiv Data Protection Commissioner* [VV], 6. oktobra 2015.

676 *Ibid.*, stav 84.

677 *Ibid.*, st. 88 i 89.

678 *Ibid.*, st. 91 i 92.

679 *Ibid.*, st. 96 i 97.

Nivo zaštite u SAD stoga nije bio „u načelu istovetan" osnovnim pravima i slobodama obezbeđenim pravom Unije[680]. SPEU je utvrdio da je povređeno više članova Povelje EU o osnovnim pravima. Za početak, povređena je suština člana 7. budući da propis SAD „omogućava javnim telima generalni pristup sadržaju elektronskih komunikacija". Zatim je prekršen i srž člana 47. jer propisom pojedincima nije pružena nikakva mogućnost korišćenja pravnih sredstava radi pristupa ličnim podacima ili radi ispravke ili brisanja ličnih podataka. Konačno, budući da su sistemom „sigurne luke" prekršeni navedeni članovi, lični podaci nisu zakonito obrađeni, što je dovelo do povrede člana 8.

Pošto je SPEU proglasio sistem „sigurne luke" nevažećim, Komisija i SAD postigli su sporazum o novom okviru, evropsko-američkom sistemu zaštite privatnosti (engl. *EU-US Privacy Shield*). Komisija je 12. jula 2016. donela odluku kojom je objavila da SAD obezbeđuje odgovarajući nivo zaštite ličnih podataka koji se prenose iz Unije u organizacije u SAD u sklopu sistema zaštite privatnosti[681].

Slično kao i sporazumom o „sigurnoj luci", okvirom evropsko-američkog sistema za zaštitu privatnosti nastoji se da se zaštite lični podaci koji se prenose iz EU u SAD u komercijalne svrhe[682]. Kompanije u SAD mogu obaviti dobrovoljno samosertifikovanje pridržavanja popisa iz sistema za zaštitu privatnosti tako što se obavežu na ispunjavanje standarda zaštite podataka tog okvira. Nadležna tela u SAD nadgledaju i proveravaju usklađenost sertifikovanih kompanija sa tim standardima.

Sistemom za zaštitu privatnosti posebno se utvrđuje sledeće:

- obaveze zaštite podataka za preduzeća koja primaju lične podatke iz EU,

680 *Ibid.*, st. 73, 74 i 96.

681 Izvršna odluka Komisije (EU) 2016/1250 od 12. jula 2016. o primerenosti zaštite u okviru evropsko-američkog sistema zaštite privatnosti u skladu s Direktivom 95/46/EZ Evropskog parlamenta i Saveta, SL L 207. Radna grupa iz člana 29. pozdravila je poboljšanja koja su uvedena tim mehanizmom zaštite privatnosti u odnosu na odluku o „sigurnoj luci", pa je pohvalila Komisiju i nadležna tela SAD jer su u završnoj verziji dokumenata o sistemu zaštite privatnosti uzeli u obzir pitanja iznesena u njenom mišljenju WP 238 o nacrtu odluke o primerenosti evropsko-američkog sistema zaštite privatnosti. Uprkos tome, istakla je niz nerešenih pitanja. Više pojedinosti dostupno je u: Radna grupa iz člana 29., *Mišljenje 01/2016 o nacrtu odluke o primerenosti evropsko-američkog sistema za zaštitu privatnosti*, doneseno 13. aprila 2016., 16/EN WP 238.

682 Više informacije dostupno je u dokumentu EU-U.S. Privacy Shield factsheet (Informativni list o evropsko-američkom sistemu za zaštitu privatnosti).

- zaštita i mogućnosti za ostvarivanje pravne zaštite pojedinaca, naročito uspostava mehanizma pravobranilaca, koji deluje nezavisno od obaveštajnih službi SAD i obrađuje tužbe pojedinaca koji smatraju da su tela SAD nadležna za nacionalnu bezbednost upotrebila njihove lične podatke na nezakonit način,

- godišnje zajedničko preispitivanje kojim se kontroliše izvršenje okvira[683]; prvo preispitivanje je održano u septembru 2017.[684]

Vlada SAD dopunila je odluku o sistemu za zaštitu privatnosti pisanim obavezama i garancijama. Njima se utvrđuju ograničenja i zaštitne mere za pristup vlade SAD ličnim podacima radi sprovođenja zakona i u svrhu nacionalne sigurnosti.

7.3.2. Prenosi koji podležu odgovarajućim zaštitnim merama

I u **pravu Unije** i u **pravu Saveta Evrope** utvrđuju se odgovarajuće zaštitne mere između rukovaoca podacima koji izvozi podatke i primaoca u trećoj zemlji ili međunarodne organizacije. Takve mere navode se kao mogući način obezbeđivanja odgovarajućeg nivoa zaštite podataka za primaoca.

U skladu sa **pravom EU**, prenosi ličnih podataka u treću zemlju ili međunarodnu organizaciju dozvoljeni su ako rukovalac podacima ili obrađivač podataka obezbeđuje odgovarajuće zaštitne mere i izvršna prava i ako su ispitanicima dostupni delotvorni pravni lekovi[685]. Popis „odgovarajućih zaštitnih mera" propisan je isključivo pravom zaštite podataka EU . Odgovarajuće zaštitne mere mogu se uspostaviti na sledeće načine:

- pravno obavezujućim i izvršnim instrumentima između tela javne vlasti ili javnih tela,

- obavezujućim korporativnim pravilima,

683 Više informacija dostupno je na internet stranici Evropske komisije o evropsko-američkom sistemu za zaštitu privatnosti.

684 Evropska komisija, *Izveštaj Komisije Evropskom parlamentu i Savetu o prvom godišnjem preispitivanju funkcionisanja evropsko-američkog sistema zaštite privatnosti*, COM(2017) 611 final, 18. oktobra 2017. Videti i Radna grupa iz člana 29., *Prvo godišnje preispitivanje funkcionisanja evropsko-američkog sistema zaštite privatnosti*¸ doneseno 28. novembra 2017., 17/EN WP 255.

685 Opšta uredba o zaštiti podataka, član 46.

- standardnim klauzulama o zaštiti podataka koje donosi Evropska komisija ili nadzorno telo,
- kodeksima ponašanja,
- mehanizmima sertifikovanja[686].

Posebne ugovorne klauzule između rukovaoca podacima ili obrađivača podataka u EU i primaoca podataka u trećoj zemlji dodatni su način obezbeđivanja odgovarajućih zaštitnih mera. Međutim, takve ugovorne klauzule mora odobriti nadležno nadzorno telo pre nego što se budu mogle primeniti kao sredstvo prenosa ličnih podataka. Isto tako, javna tela mogu iskoristiti odredbe o zaštiti podataka uvršćene u njihove administrativne dogovore ako ih nadzorno telo odobri[687].

U skladu sa pravom Saveta Evrope, prenosi podataka u državu ili međunarodnu organizaciju koja nije ugovorna strana modernizovane Konvencije br. 108 dopušteni su pod uslovom da se obezbedi odgovarajući nivo zaštite. To se može postići:

- zakonom države ili međunarodne organizacije ili
- *ad hoc* ili standardizovanim zaštitnim merama ugrađenim u pravno obavezujući dokument[688].

Prenosi koji podležu ugovornim klauzulama

I u **pravu Saveta Evrope** i u **pravu EU** utvrđuju se ugovorne klauzule kojima se vezuju rukovalac podacima koji izvozi podatke i primalac u trećoj zemlji. Takve klauzule navode se kao mogući način obezbeđivanja odgovarajućeg nivoa zaštite podataka za primaoca[689].

Na **nivou EU**, Evropska komisija uz pomoć Radne grupe iz člana 29. razvila je standardne klauzule o zaštiti podataka koje su službeno overene odlukom Komisije kao

686 Opšta uredba o zaštiti podataka, član 46. stav 1. tačke (c) i (d), član 46. stav 2. tačke (a), (b), (e) i (f) i član 47.

687 *Ibid*., član 46. stav 3.

688 Modernizovana Konvencija br. 108, član 14. stav 3. tačka (b).

689 Opšta uredba o zaštiti podataka, član 46. stav 3; modernizovana Konvencija br. 108, član 14. stav 3. tačka (b).

dokaz odgovarajućeg nivoa zaštite podataka[690]. Budući da su odluke Komisije u celini obavezujuće u državama članicama, domaća tela nadležna za nadzor prenosa podataka moraju potvrditi te standardne ugovorne klauzule u svojim postupcima[691]. Zato, ako se rukovalac podacima koji izvozi podatke i primalac iz treće zemlje dogovore i potpišu te klauzule, to bi za nadzorno telo trebalo da bude dovoljan dokaz sprovođenja odgovarajućih zaštitnih mera. Međutim, u predmetu *Schrems* SPEU je smatrao da Evropska komisija nije nadležna za ograničenje ovlašćenja nacionalnih nadzornih tela da kontrolišu prenos ličnih podataka u treću zemlju koja je bila predmet odluke Komisije o primerenosti[692]. Zato se domaća nadzorna tela ne sprečavaju da izvršavaju svoja ovlašćenja, uključujući ovlašćenje da suspenduju ili zabrane prenos ličnih podataka kada se prenosom krši zakonodavstvo EU ili domaće zakonodavstvo o zaštiti podataka, na primer, kada se uvoznik podataka ne pridržava standardnih ugovornih klauzula[693].

Postojanje standardnih klauzula o zaštiti podataka u pravnom okviru EU ne sprečava rukovaoce podacima da utvrde druge *ad hoc*, pojedinačne ugovorne klauzule, pod uslovom da ih odobri nadležno nadzorno telo[694]. Međutim, tim klauzulama bi trebalo da obezbede jednak nivo zaštite koji obezbeđuju standardne klauzule o zaštiti podataka. Prilikom odobravanja *ad hoc* klauzula, nadzorna tela moraju da primene mehanizam doslednosti kako bi se osigurao dosledan regulatorni pristup na nivou EU[695]. To znači da nadležno nadzorno telo mora da obavesti EOZP o svom nacrtu odluke o klauzulama. EOZP će o tome dati mišljenje, a nadzorno telo mora u najvećoj mogućoj meri da uzme u obzir to mišljenje prilikom donošenja odluke. Ako telo ne namerava da sledi mišljenje EOZP-a, aktiviraće se mehanizam rešavanja sporova unutar EOZP-a i Odbor će doneti obavezujuću odluku[696].

690 *Ibid*., član 46. stav 2. tačka (b) i član 46. stav 5.

691 *Ibid*., član 46. stav 2. tačka (c); Ugovor o funkcionisanju Evropske unije, član 288.

692 SPEU, C-362/14, *Maximillian Schrems protiv Data Protection Commissioner* [VV], 6. oktobra 2015, st. od 96 do 98 i od 102 do 105.

693 Kako bi uzela u obzir stav SPEU u predmetu *Schrems*, Komisija je izmenila svoju Odluku o standardnim ugovornim klauzulama. Izvršna odluka Komisije (EU) 2016/2297 od 16. decembra 2016. o izmeni odluka 2001/497/EZ i 2010/87/EU o standardnim ugovornim klauzulama za prenos ličnih podataka u treće zemlje i obrađivačima u tim zemljama u skladu s Direktivom 95/46/EZ Evropskog parlamenta i Saveta, SL 2016 L344.

694 Opšta uredba o zaštiti podataka, član 46. stav 3. tačka (a).

695 *Ibid*., član 63. i član 64. stav 1. tačka (e).

696 *Ibid*., član 64. i član 65.

Najvažnije osobine standardnih ugovornih klauzula jesu:

- klauzula o korisniku, trećoj strani, kojom se ispitanicima omogućava ostvarivanje ugovornih prava iako nisu strane ugovora,

- primalac ili uvoznik podataka pristaje na podvrgavanje ovlašćenju domaćeg nadzornog tela i/ili sudova rukovaoca podacima koji izvozi podatke u slučaju spora.

Dostupne su dve grupe standardnih klauzula za prenose između dva rukovaoca podacima koje rukovalac podacima može odabrati[697]. Za prenose između rukovaoca podacima i obrađivača podataka postoji samo jedna grupa standardnih ugovornih klauzula[698]. Međutim, te standardne ugovorne klauzule trenutno su predmet sudskog postupka.

Primer: Nakon što je SPEU proglasio odluku o „sigurnoj luci" nevažećom[699], prenosi ličnih podataka u SAD više se ne mogu zasnivati na toj odluci o primerenosti. Tokom pregovora sa telima SAD i u očekivanju donošenja nove odluke o primerenosti (koja je konačno donesena 12. jula 2016.)[700], prenosi su se mogli vršiti samo na osnovu drugih pravnih osnova, kao što su standardne ugovorne klauzule ili obavezujuća korporativna pravila. Nekoliko kompanija, uključujući kmpaniju Fejsbuk Irska (protiv koje je pokrenut predmet koji je doveo do poništavanja Odluke o „sigurnoj luci"), počelo je da primenjuje standardne ugovorne klauzule kako bi nastavile da prenose podatke između EU i SAD.

---

697 Grupa I nalazi se u Prilogu Odluci Komisije 2001/497/EZ od 15. juna 2001. (Evropska komisija (2001)) o standardnim ugovornim klauzulama za prenos ličnih podataka u treće zemlje, u skladu s Direktivom 95/46/EZ, SL 2001 L 181; grupa II nalazi se u Prilogu Odluci Komisije 2004/915/EZ od 27. decembra 2004. (Evropska komisija (2004)) o izmeni Odluke 2001/497/EZ u pogledu uvođenja alternativne grupe standardnih ugovornih klauzula za prenos ličnih podataka u treće zemlje, SL 2004 L 385.

698 Evropska komisija (2010), Odluka Komisije 2010/87/EU od 5. februara 2010. o standardnim ugovornim klauzulama za prenos ličnih podataka obrađivačima u trećim zemljama u skladu s Direktivom 95/46/EZ Evropskog parlamenta i Saveta, SL 2010 L 39. U trenutku izrade priručnika, upotreba standardnih ugovornih klauzula kao osnove za prenose ličnih podataka u SAD bila je predmet sudskog postupka pred irskim Visokim sudom.

699 SPEU, C-362/14, *Maximillian Schrems protiv Data Protection Commissioner* [VV], 6. oktobra 2015.

700 Izvršna odluka Komisije (EU) 2016/1250 od 12. jula 2016. o primerenosti zaštite u okviru evropsko-američkog sistema zaštite privatnosti u skladu s Direktivom 95/46/EZ Evropskog parlamenta i Saveta, SL L 207.

G. Šrems je podneo tužbu irskom nadzornom telu, zatraživši da obustavi prenose podataka u SAD na osnovu standardnih ugovornih klauzula. U osnovi je tvrdio da prilikom prenosa njegovih ličnih podataka iz irske podružnice kompanije Fejsbuk kompaniji Fejsbukk sa sedištem u SAD, kao i na servere koji su smešteni u SAD, nije obezbeđena njihova zaštita. Kompanija Fejsbuk sa sedištem u SAD obavezana je zakonima SAD prema kojima bi mogla da bude dužna da otkrije lične podatke policijskim organima u SAD, a evropski građani nemaju na raspolaganju nikakav pravni lek protiv takve prakse[701]. Zbog toga je SPEU zaključio da je Odluka o „sigurnoj luci" nevažeća, a iako je presuda Suda bila ograničena na preispitivanje te odluke, tužilac je smatrao da su postavljena pitanja relevantna i za prenos koji se zasniva na ugovornim klauzulama. U trenutku izrade priručnika, predmet je razmatrao irski Visoki sud. Čini se da tužilac namerava da pokrene postupak pred SPEU kako bi osporio valjanost odluke Evropske komisije o standardnim ugovornim klauzulama. Kao što je opisano u poglavlju 5, samo SPEU ima ovlašćenje da proglasi neki instrument EU nevažećim.

Prenosi koji podležu obavezujućim korporativnim pravilima

Pravom EU dopuštaju se i prenosi ličnih podataka na osnovu obavezujućih korporativnih pravila za međunarodne prenose koji se odvijaju unutar iste grupe preduzeća ili preduzeća koja se bave zajedničkom ekonomskom delatnošću[702]. Pre nego što obavezujuća korporativna pravila mogu da se primene kao sredstvo prenosa ličnih podataka, nadležno nadzorno telo mora da ih odobri u skladu s obavezujućim korporativnim pravilima, služeći se mehanizmom konzistentnosti.

Da bi bila odobrena, obavezujuća korporativna pravila moraju da budu pravno obavezujuća, obuhvataju sva temeljna načela zaštite podataka tako da se moraju primenjivati na sve članove grupe, koji su dužni da ih izvršavaju. Njima se moraju izričito dodeliti izvršna prava ispitanicima, ona moraju da uključuju sva temeljna načela zaštite podataka i da budu u skladu s određenim službenim zahtevima, kao što su navođenje strukture preduzeća, opisivanje prenosa i načina primene načela zaštite podataka. To uključuje davanje odgovarajućih informacija ispitanicima. Obavezuju-

701 Više informacija potražite u revidiranoj tužbi (dostupnoj na engleskom jeziku) protiv kompanije Facebook Ireland Ltd, koju je g. Maximillian Schrems podneo irskom Povereniku za zaštitu podataka 1. decembra 2015.

702 Opšta uredba o zaštiti podataka, član 47.

ćim korporativnim pravilima moraju se, između ostalog, utvrditi prava ispitanika i odredbe o odgovornosti za svako kršenje pravila[703]. Prilikom odobravanja obavezujućih korporativnih pravila aktiviraće se mehanizam konzistentnosti za saradnju nadzornih tela (opisan u poglavlju 5).

U okviru mehanizma doslednosti, vodeće nadzorno telo preispituje predložena obavezujuća korporativna pravila, donosi nacrt odluke i o tome obaveštava EOZP. Odbor daje mišljenje o tom predmetu, a vodeće nadzorno telo može službeno da odobri obavezujuća korporativna pravila dok „što je više moguće uzima u obzir" mišljenje Odbora. To mišljenje nije pravno obavezujuće, ali ako nadzorno telo namerava da ga zanemari, aktiviraće se mehanizam za rešavanje sporova, a Odbor bi trebalo da donese pravno obavezujuću odluku dvotrećinskom većinom članova[704].

Prema **pravu Saveta Evrope**, *ad hoc* ili standardizovane zaštitne mere, koje su ugrađene u pravno obavezujući dokument[705], takođe uključuju obavezujuća korporativna pravila.

7.3.3. Odstupanja u posebnim situacijama

Unutar prava EU prenosi ličnih podataka u treće zemlje mogu biti opravdani čak i u nedostatku odgovarajuće odluke ili zaštitnih mera, kao što su standardne ugovorne klauzule ili obavezujuća korporativna pravila, u bilo kom od sledećih slučajeva:

- ispitanik izričito pristaje na prenos podataka,
- ispitanik sklapa ili se priprema da sklopi ugovorni odnos u sklopu kojeg je nužan prenos podataka u inostranstvo,
- sklapanje ugovora između rukovaoca podacima i treće strane u interesu ispitanika,
- važni razlozi javnog interesa,
- postavljanje, ostvarivanje ili odbrana pravnih zahteva,
- zaštita životno važnih interesa ispitanika,

703 Detaljan opis dostupan je u Opštoj uredbi o zaštiti podataka, član 47.

704 *Ibid*., član 57. stav 1. tačka (s), član 58. stav 1. tačka (j), član 64. stav 1. tačka (f), član 65. stavovi 1. i 2.

705 Modernizovana Konvencija br. 108, član 14. stav 3. tačka (b).

- prenos podataka iz javnih registara (radi se o prevladavajućim interesima javnosti koji se tiču pristupa informacijama čuvanim u javnim registrima)[706].

Ako se ne primenjuje nijedan od ovih uslova, a prenosi se ne mogu zasnivati na odluci o primerenosti ili odgovarajućim zaštitnim merama, prenos se može ostvariti samo ako se ne ponavlja, ako se odnosi samo na ograničen broj ispitanika pa je nužan za potrebe uverljivih, legitimnih interesa rukovaoca podacima, pod uslovom da oni nisu podređeni pravima ispitanika[707]. U tim slučajevima rukovalac podacima mora da proceni okolnosti prenosa i odredi zaštitne mere. Takođe mora da obavesti nadzorno telo i dotične ispitanike o prenosu i o legitimnim interesima kojima ga opravdava.

Činjenica da su odstupanja krajnja mera za zakonite prenose[708] (koja se primenjuju samo u slučaju nedostatka odluke o primerenosti i drugih zaštitnih mera) pokazuje koliko su ona izuzetna, a dodatno je naglašeno u uvodnim izjavama OUZP-a[709]. Stoga se odstupanja prihvataju kao mogućnost „prenosa u određenim okolnostima" na osnovu pristanka i kada je „prenos povremen i nužan"[710] u vezi sa ugovorom ili pravnim zahtevom.

Usto, u skladu sa smernicama Radne grupe iz člana 29., oslanjanje na odstupanja u posebnim situacijama mora biti izuzetak, zasnivati se na pojedinačnim slučajevima i ne sme se primenjivati na masovne ili ponavljajuće prenose[711]. Evropski nadzornik za zaštitu podataka takođe je naglasio da odstupanja treba da budu izuzetak kada se primenjuju kao pravna osnova za prenose na osnovu Uredbe 45/2001, napominjući da to rešenje treba da se primenjuje „u ograničenim slučajevima" i „za povremene prenose"[712].

706 Opšta uredba o zaštiti podataka, član 49.

707 *Ibid.*

708 *Ibid*., član 49. stav 1.

709 Videti Opštu uredbu o zaštiti podataka, član 49. stav 1. tačke (a), (b) i (e) i uvodnu izjavu 113.

710 *Ibid*., član 49. stav 1.

711 Radna grupa iz člana 29. (2005), Radni dokument o zajedničkom tumačenju člana 26. stav 1. Direktive 95/46/EZ od 24. oktobra 1995, WP 114, Bruxelles, 25. novembra 2005.

712 Evropski nadzornik za zaštitu podataka, *The transfer of personal data to third countries and international organisations by EU institutions and bodies* (Prenos ličnih podataka u treće zemlje ili međunarodne organizacije koji vrše institucije i tela EU), Dokument o stajalištu, Bruxelles, 14. jula 2014., str. 15.

Primer: Kompanija koja pruža usluge globalnog distribucionog sistema (GDS), sa sedištem u SAD, stavlja na raspolaganje mrežni sistem za rezervacije većem broju avio-kompanija, hotela i brodova za krstarenje širom sveta i obrađuje podatke za desetine miliona osoba u EU. Za prvobitni prenos podataka na njegove servere u SAD kompanija koja pruža usluge GDS oslanja se na odstupanje kao zakonitu osnovu za prenose, odnosno na nužnost sklapanja ugovora. Stoga se ne poziva ni na kakve druge zaštitne mere za lične podatke koji potiču iz Evrope, prenose se u SAD i zatim distribuiraju hotelima širom sveta (što znači da nema zaštitnih mera ni za dalje prenose). Kompanija koja pruža GDS ne pridržava se zahteva iz OUZP-a za zakonite međunarodne prenose, podataka jer se oslanja na odstupanje kao zakonitu osnovu za masovne prenose.

Ako odluka o primerenosti nije donesena, EU ili njegove države članice smeju da utvrde ograničenja prenosa pojedinih kategorija ličnih podataka trećoj zemlji, uprkos ispunjavanju drugih uslova za takve prenose, iz razloga javnog interesa. Takva ograničenja treba da se smatraju izuzecima, a države članice moraju o odgovarajućim odredbama da obaveste Komisiju[713].

Pravom Saveta Evrope dopušta se prenos podataka na oblasti koja nemaju odgovarajuću zaštitu podataka u sledećim slučajevima:

- ispitanik je dao pristanak,
- interesi ispitanika uslovljavaju takav prenos,
- prisutni su prevladavajući legitimni interesi, naročito važni javni interesi, propisani zakonom,
- to je nužna i srazmerna mera u demokratskom društvu[714].

7.3.4. Prenosi koji se zasnivaju na međunarodnim sporazumima

EU može da sklapa međunarodne sporazume s trećim zemljama kojima se uređuje prenos ličnih podataka u posebne svrhe. Ti sporazumi moraju da sadrže odgovarajuće

713 Videti Opštu uredbu o zaštiti podataka, član 49. stav 5.

714 Modernizovana Konvencija br. 108, član 14. stav 4.

zaštitne mere kako bi se obezbedila zaštita ličnih podataka dotičnih pojedinaca. OUZP-om se ne dovode u pitanje ti međunarodni sporazumi[715].

Države članice mogu takođe sklopiti međunarodne sporazume sa trećim zemljama ili međunarodnim organizacijama koje obezbeđuju odgovarajuću nivo zaštite osnovnih prava i sloboda pojedinaca, u meri u kojoj ti sporazumi ne utiču na primenu OUZP-a.

Slično je pravilo propisano članom 12. stav 3. tačka (a) modernizovane Konvencije br. 108.

Primeri međunarodnih sporazuma koji se odnose na prenos ličnih podataka su sporazumi o evidencijama podataka o putnicima (EPP).

Evidencija podataka o putnicima

Avio-kompanije u postupku rezervacije letova prikupljaju podatke iz evidencije podataka o putnicima koji, između ostalog, uključuju imena, adrese, podatke o kreditnoj kartici, kao i brojeve sedišta putnika. Avio-kompanije prikupljaju te podatke i za sopstvene komercijalne potrebe. Evropska unija sklopila je sporazume s određenim trećim zemljama (Australijom, Kanadom i SAD) o prenosu podataka iz evidencije podataka o putnicima radi sprečavanja, otkrivanja, istrage i gonjenja terorističkih napada ili ozbiljnog transnacionalnog kriminala. Unija je 2016. takođe donela Direktivu (EU) 2016/861, poznatu i kao Direktiva EU o evidenciji podataka o putnicima[716]. Tom Direktivom se utvrđuje pravni okvir za države članice EU koji se odnosi na prenos podataka iz evidencija podataka o putnicima nadležnim telima u trećim zemljama, takođe kako bi se sprečili, otkrili, istraživali ili gonili teroristički napadi i ozbiljna krivična dela. Prenosi podataka iz evidencija nadležnim telima trećih zemalja razlikuju se u zavisnosti od slučaja i podležu pojedinačnoj proceni nužnosti prenosa za svrhe navedene u Direktivi i poštovanju osnovnih prava.

Usklađenost sporazuma o evidencijama podataka o putnicima između EU i trećih zemalja s osnovnim pravima na privatnost i zaštitu podataka koja su garantovana Poveljom EU o osnovnim pravima dovodila se u pitanje u prošlosti. Kada je EU nakon pregovora sa Kanadom 2014. potpisala sporazum o prenosu i obradi podataka iz evidencije podataka o putnicima, Evropski parlament je odlučio da prosledi SPEU predmet upoređivanja zakonitosti sporazuma sa pravom EU, naročito s obzirom na članove 7. i 8. Povelje.

715 Opšta uredba o zaštiti podataka, uvodna izjava 102.

716 Direktiva (EU) 2016/681 Evropskog parlamenta i Saveta od 27. aprila 2016. o upotrebi podataka iz evidencije podataka o putnicima (PNR) u svrhu sprečavanja, otkrivanja, istrage i krivičnog gonjenja krivičnih dela terorizma i teških krivičnih dela, SL 2016 L 119.

Primer: U Mišljenju o zakonitosti sporazuma o evidenciji podataka o putnicima između EU i Kanade[717] SPEU je smatrao da predviđeni sporazum u tadašnjem obliku nije usklađen s osnovnim pravima koja su garantovana Poveljom, pa se zato ne može zaključiti. Budući da je uključivao obradu ličnih podataka, predstavljao je mešanje u pravo na zaštitu ličnih podataka koje je garantovano članom 8. Povelje. Istovremeno je predstavljao i ograničenje prava na poštovanje privatnog života, utvrđeno u članu 7., budući da se, gledano u celini, podaci iz EPP mogu grupisati i analizirati na način koji bi otkrio putne navike, odnose među pojedincima, informacije o njihovom finansijskom statusu, prehrambene navike i zdravstveno stanje, čime bi se umešalo u privatne živote pojedinaca.

Mešanje u osnovna prava koje bi predviđeni sporazum prouzrokovao odnosilo se na cilj od opšteg interesa, tačnije javnu bezbednost i borbu protiv terorizma i ozbiljnog transnacionalnog kriminala. Međutim, SPEU je podsetio da takvo mešanje mora biti ograničeno na ono što je strogo nužno za postizanje predviđenog cilja da bi bilo opravdano. Posle preispitivanja odredbi predviđenog sporazuma, SPEU je zaključio da ne ispunjava kriterijum „strogo nužnog". Između ostalog, u donošenju tog zaključka SPEU je razmatrao sledeće činioce:

- činjenicu da je predviđeni sporazum podrazumevao prenos osetljivih podataka. Podaci iz evidencije podataka o putnicima, prikupljeni u skladu sa predviđenim sporazumom, mogli su da uključuju osetljive podatke koji otkrivaju rasno ili etničko poreklo, verska uverenja ili zdravstveno stanje putnika. Prenos i obrada osetljivih podataka, koje su vršila kanadska nadležna tela, mogli su predstavljati rizik za načelo nediskriminacije, pa su zato zahtevali precizno i uverljivo opravdanje na osnovu osnove koja nije javna sigurnost ili borba protiv ozbiljnog kriminala. Predviđeni sporazum nije pružio takvo opravdanje[718],
- Sud je smatrao da neprekidno čuvanje podataka iz evidencije podataka o putnicima tokom perioda od pet godina, čak i nakon odlaska putnika iz Kanade, takođe prelazi granice strogo nužnog. SPEU je smatrao da bi se kanadskim nadležnim telima moglo dopustiti zadržavanje podataka o putnicima za koje objektivni dokazi ukazuju da bi mogli predstavljati pretnju javnoj sigurnosti, čak i nakon što te osobe napuste Kanadu. Ali, čuvanje ličnih podataka *svih* putnika, za koje ne postoje čak ni posredni dokazi da predstavljaju pretnju javnoj bezbednosti, nije bila opravdana[719].

717 SPEU, *Mišljenje 1/15 Suda (veliko Veće)*, 26. jula 2017.

718 *Ibid.*, stav 165.

719 *Ibid.*, st. od 204 do 207.

Savetodavni odbor Konvencije br. 108 dao je mišljenje o implikacijama sporazuma o evidencijama podataka o putnicima za zaštitu podataka na osnovu prava Saveta Evrope[720].

Podaci o porukama

Belgijsko Društvo za svetsku međubankovnu finansijsku telekomunikaciju (SWIFT), koje obrađuje većinu globalnih prenosa novca iz evropskih banaka, poslovalo je putem „oglednog" centra u SAD pa je primilo zahtev za otkrivanje podataka Ministarstvu finansija SAD u svrhu istrage terorizma u sklopu njegovog Programa za praćenje finansiranja terorizma[721].

Sa gledišta EU, nije postojala primerena pravna osnova za otkrivanje tih podataka, koji su se uglavnom odnosili na građane EU, u SAD samo zato što je tamo bio smešten jedan od SWIFT-ovih centara za obradu podataka.

Poseban sporazum između EU i SAD, poznat kao Sporazum o SWIFT-u, sklopljen je 2010. godine kako bi se obezbedila potrebna pravna osnova i odgovarajući standardi zaštite podataka[722].

Prema tom sporazumu, finansijski podaci koje čuva SWIFT i dalje se dostavljaju Ministarstvu finansija SAD u svrhu sprečavanja, istrage, otkrivanja ili gonjenja terorizma ili finansiranja terorističkih aktivnosti. Ministarstvo finansija SAD može od SWIFT-a zatražiti finansijske podatke pod uslovom da:

- su finansijski podaci u zahtevu što jasnije utvrđeni,
- je u zahtevu jasno potkrepljena nužnost podataka,

720 Savet Evrope, *Opinion on the Data protection implications of the processing of Passenger Name Records* (Mišljenje o implikacijama obrade evidencija imena putnika za zaštitu podataka), T-PD(2016)18rev, 19. avgusta 2016.

721 U tom kontekstu videti: Radna grupa iz člana 29. (2011), Mišljenje 14/2011 o pitanjima zaštite podataka u vezi sa sprečavanjem pranja novca i finansiranja terorizma, WP 186, Bruxelles, 13. juna 2011.; Radna grupa iz člana 29. (2006), Mišljenje 10/2006 o obradi ličnih podataka koju vrši Društvo za svetsku međubankovnu finansijsku telekomunikaciju (SWIFT), WP 128, Bruxelles, 22. novembra 2006.; belgijska Komisija za zaštitu privatnosti (Commission de la protection de la vie privée) (2008), „Postupak kontrole i preporuke pokrenut spram društva SWIFT scrl", Odluka, 9. decembra 2008.

722 Odluka Saveta 2010/412/EU od 13. jula 2010. o sklapanju Sporazuma između Evropske unije i Sjedinjenih Američkih Država o obradi i slanju podataka o izveštajima u vezi sa finansijskim plaćanjima iz Evropske unije Sjedinjenim Američkim Državama za potrebe Programa za praćenje finansiranja terorističkih delatnosti, SL 2010 L 195, str. 3 i 4. Tekst Sporazuma priložen je toj odluci, SL 2010 L 195, str. 5–14.

- je zahtev što precizniji kako bi se smanjila količina zatraženih podataka,

- se u zahtevu ne traže podaci koji se odnose na Jedinstveno područje plaćanja u evrima (JPPE)[723].

Europol mora primiti primerak svakog zahteva Ministarstva finansija SAD i potvrditi da li se poštuju načela Sporazuma o SWIFT-u[724]. Ako se potvrdi da se poštuju, SWIFT mora finansijske podatke da dostavi direktno Ministarstvu finansija SAD. Ministarstvo mora čuvati finansijske podatke u bezbednom fizičkom okruženju tako da im mogu pristupiti samo analitičari koji istražuju terorizam ili njegovo finansiranje, a finansijski podaci ne smeju biti međusobno povezani ni sa kojom drugom bazom podataka. Generalno se finansijski podaci primljeni od SWIFT-a moraju izbrisati najkasnije pet godina od prijema. Finansijski podaci koji su bitni za određene istrage ili gonjenja mogu se zadržati sve dok su nužni za te istrage ili gonjenja.

Ministarstvo finansija SAD može preneti informacije iz podataka primljenih od SWIFT-a određenim telima policije, javne bezbednosti ili suzbijanja terorizma, unutar ili izvan SAD, isključivo radi istrage, otkrivanja, sprečavanja ili gonjenja terorizma i njegovog finansiranja. Ako dalji prenos finansijskih podataka uključuje građanina ili stanovnika države članice Evropske unije, svaka razmena podataka sa telima treće zemlje podleže prethodnom pristanku nadležnih tela predmetne države članice. Mogu se napraviti izuzeci ako je razmena podataka nužna za sprečavanje neposredne i ozbiljne pretnje javnoj sigurnosti.

Nezavisna tela koja vrše nadzor, uključujući osobu koju imenuje Evropska komisija, nadgledaju usklađenost sa načelima Sporazuma o SWIFT-u. Ona mogu u stvarnom vremenu i retroaktivno pregledati sve pretrage datih podataka, zatražiti dodatne informacije za opravdanje linkova tih pretraga sa terorizmom i blokirati bilo koje ili sve pretrage kojima se krše zaštitne mere utvrđene Sporazumom.

723 *Ibid*., član 4. stav 2.

724 Zajedničko nadzorno telo Europola sprovelo je revizije Europolovih aktivnosti u tom području.

Ispitanici imaju pravo da dobiju potvrdu nadležnog nadzornog tela EU za zaštitu podataka da se poštuju njihova prava na zaštitu podataka. Ispitanici takođe imaju pravo na ispravku, brisanje ili blokiranje svojih podataka koje je prikupilo i sačuvalo Ministarstvo finansija SAD u skladu sa Sporazumom o SWIFT-u. Međutim, prava na pristup ispitanika mogu podlegati određenim pravnim ograničenjima. Ako mu je pristup odbijen, ispitanika treba pisanim putem obavestiti o odbijanju i o njegovom pravu na pravni lek u vidu upravnog i sudskog postupka u SAD.

Sporazum o SWIFT-u važi pet godina, a prvi period važenja trajao je do avgusta 2015. Automatski se produžuje na period od još jedne godine, osim ako jedna od strana obavesti drugu najmanje šest meseci unapred o svojoj nameri da ne produži sporazum. Automatsko produženje obavljeno je u avgustu 2015, 2016. i 2017, a njime se obezbeđuje važnost Sporazuma o SWIFT-u barem do avgusta 2018.[725]

725 *Ibid.*, član 23. stav 2.

8

Zaštita podataka u kontekstu policije i krivičnog pravosuđa

EU	Obuhvaćena pitanja	Savet Evrope
Direktiva o zaštiti podataka za policiju i tela krivičnog pravosuđa	**Uopšteno**	Modernizovana Konvencija br. 108
	Policija	Police Recommendation (Preporuka o policiji) Practical Guide on the use of personal data in the police sector (Praktični vodič o upotrebi ličnih podataka u sektoru policije)
	Nadzor	ESLJP, *B. B. protiv Francuske*, br. 5335/06, 2009. ESLJP, *S. i Marper protiv Ujedinjenog Kraljevstva* [VV], br. 30562/04 i 30566/04, 2008. ESLJP, *Allan protiv Ujedinjenog Kraljevstva*, br. 48539/99, 2002. ESLJP, *Malone protiv Ujedinjenog Kraljevstva*, br. 8691/79, 1984. ESLJP, *Klass i drugi protiv Nemačke*, br. 5029/71, 1978. ESLJP, *Szabó i Vissy protiv Mađarske*, br. 37138/14, 2016. ESLJP, *Vetter protiv Francuske*, br. 59842/00, 2005.
	Kibernetički kriminal	Cybercrime Convention (Konvencija o kibernetičkom kriminalu)

EU	Obuhvaćena pitanja	Savet Evrope
Ostali specifični pravni instrumenti		
Prumska odluka	**Za posebne podatke: otiske prstiju, DNK, huliganstvo, podatke o putnicima u vazdušnom saobraćaju, telekomunikacione podatke itd.**	Modernizovana Konvencija br. 108, član 6. Preporuka o policiji, *Practical Guide on the use of personal* data in the police sector (Praktični vodič o upotrebi ličnih podataka u sektoru policije)
Švedska inicijativa (Okvirna odluka Saveta 2006/960/PUP)	**Pojednostavljenje razmene informacija i obaveštajnih podataka među policijskim organima**	ESLJP, *S. i Marper protiv Ujedinjenog Kraljevstva* [VV], br. 30562/04 i 30566/04, 2008.
Direktiva (EU) 2016/681 o upotrebi podataka iz evidencije podataka o putnicima (PNR) u svrhu sprečavanja, otkrivanja, istrage i krivičnog gonjenja krivičnih dela terorizma i teških krivičnih dela SPEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland* i *Kärntner Landesregierung i dr.* [VV], 2014. SPEU, spojeni predmeti C-203/15 i C-698/15, *Tele2 Sverige* i *Home Department protiv Toma Watsona i drugih* [VV], 2016.	**Zadržavanje ličnih podataka**	ESLJP, *B. B. protiv Francuske*, br. 5335/06, 2009.
Uredba o Europolu Odluka o Eurojust-u	**Posebne agencije**	Preporuka o policiji
Odluka o Šengenskom informacionom sistemu II Uredba o VIS-u Uredba o Eurodac-u CIS Decision (Odluka o CIS-u)	**Posebni zajednički informacioni sistemi**	Preporuka o policiji ESLJP, *Dalea protiv Francuske*, br. 964/07, 2010.

Radi uravnoteženja interesa pojedinca u pogledu zaštite podataka i interesa društva u pogledu prikupljanja podataka radi suzbijanja zločina i obezbeđenja nacionalne i javne bezbednosti, Savet Evrope i Evropska unija doneli su posebne pravne instrumente. U ovom delu daje se pregled prava Saveta Evrope (deo 8.1) i EU (deo 8.2) koje se odnosi na zaštitu podataka u poslovima policije i krivičnog pravosuđa.

8.1. Pravo Saveta Evrope u oblasti zaštite podataka, nacionalne bezbednosti, policije i krivičnog pravosuđa

Ključne tačke

- Modernizovana Konvencija br. 108 i Preporuka o policiji Saveta Evrope odnose se na zaštitu podataka u svim područjima delovanja policije.
- Konvencija o sajber kriminalu (Budimpeštanska konvencija) obavezujući je međunarodni pravni instrument koji se odnosi na krivična dela počinjena nad elektronskim mrežama i putem njih. Takođe je važna za istragu nekibernetičkih krivičnih dela koja uključuju elektronske uređaje.

Jedna značajna razlika između prava Saveta Evrope i EU je ta što se **pravo Saveta Evrope** primenjuje i na oblast nacionalne bezbednosti. To znači da ugovorne strane moraju da se pridržavaju oblasti primene člana 8. EKLJP-a čak i u aktivnostima u vezi sa nacionalnom bezbednošću. Nekoliko presuda ESLJP-a odnosilo se na državne aktivnosti u osetljivim oblastima zakonodavstva i prakse u vezi sa nacionalnom bezbednošću[726].

U pogledu policije i krivičnog pravosuđa na evropskom nivou, modernizovanom Konvencijom br. 108 obuhvaćene su sve oblasti obrade ličnih podataka, a svrha njenih odredbi uopšteno je da se uredi obrada ličnih podataka. Stoga se modernizovana Konvencija br. 108 odnosi na zaštitu podataka u oblasti policije i krivičnog pravosuđa. Obrada genetskih podataka, ličnih podataka u vezi sa krivičnim delima, krivičnim postupcima i presudama, kao i svim povezanim bezbednosnim merama, biometrijskih podataka koji služe za identifikaciju osobe i svih osetljivih ličnih poda-

726 Videti, na primer, ESLJP, *Klass i drugi protiv Nemačke*, br. 5029/71, 6. septembra 1978.; ESLJP, *Rotaru protiv Rumunije* [VV], br. 28341/95, 4. maja 2000. i ESLJP, *Szabó i Vissy protiv Mađarske*, br. 37138/14, 12. januara 2016.

taka, dopuštena je samo kada su uspostavljene odgovarajuće zaštitne mere protiv rizika koje obrada takvih podataka može prouzrokovati za interese, prava i osnovne slobode ispitanika, a najviše rizika od diskriminacije[727].

Pravni zadaci policije i tela krivičnog pravosuđa često zahtevaju obradu ličnih podataka koja može imati ozbiljne posledice za dotične pojedince. Preporuka o policiji, koju je Savet Evrope doneo 1987. godine, pruža državama članicama Saveta Evrope smernice o načinu izvršenja načela Konvencije br. 108 u kontekstu obrade ličnih podataka koju vrše policijska tela[728]. Preporuka je dopunjena praktičnim vodičem o upotrebi ličnih podataka u sektoru policije, koji je doneo Savetodavni odbor Konvencije br. 108[729].

Primer: U predmetu *D. L. protiv Bugarske*[730] socijalna služba je smestila je podnosioca predstavke u zaštićenu obrazovnu ustanovu u skladu sa sudskim nalogom. Sva pisana korespondencija i telefonski razgovori podvrgnuti su opštem i neselektivnom nadzoru ustanove. ESLJP je smatrao da je povređen član 8. jer dotična mera nije bila nužna u demokratskom društvu. ESLJP je naveo da se mora preduzeti sve što je moguće kako bi se maloletnicima smeštenima u ustanovu omogućio dovoljan kontakt sa spoljašnjim svetom, jer je to neophodno za njihovo pravo na ophođenje sa dostojanstvom i od ključne važnosti za pripremu njihovog ponovnog integrisanja u društvo. To se podjednako odnosilo na posete i na pisanu korespondenciju ili telefonske razgovore. Zatim, u vršenju nadzora nije se pravila razlika između komunikacije sa članovima porodice i komunikacije sa NVO koje zastupaju prava dece ili advokatima. Osim toga, odluka o presretanju komunikacije nije bila utemeljena na pojedinačnoj analizi rizika u svakom pojedinom slučaju.

Primer: U predmetu *Dragojević protiv Hrvatske*[731] podnosilac je bio osumnjičen za krijumčarenje droge. Proglašen je krivim pošto je istražni sudija odobrio primenu mera tajnog nadzora kako bi se presreli njegovi telefonski pozivi. ESLJP je smatrao da je ta mera, u vezi sa kojom je podneta predstavka, predstavljala

727 Modernizovana Konvencija br. 108, član 6.

728 Savet Evrope, Komitet ministara (1987.), Preporuka Rec(87)15 državama članicama o upotrebi ličnih podataka u policijskom sektoru, 17. septembra 1987.

729 Savet Evrope (2018.), Savetodavni odbor Konvencije br. 108, „Practical Guide on the use of personal data in the police sector" (Praktični vodič o upotrebi ličnih podataka u sektoru policije), T-PD(2018)1.

730 ESLJP, *D. L. protiv Bugarske*, br. 7472/14, 19. maja 2016.

731 ESLJP, *Dragojević protiv Hrvatske*, br. 68955/11, 15. januara 2015.

mešanje u pravo na poštovanje privatnog života i prepiske. Odobrenje istražnog sudije zasnivalo se isključivo na izjavi tužilaštva da se „istraga nije mogla izvršiti drugim sredstvima". ESLJP je takođe istakao da su krivični sudovi ograničili svoju procenu o primeni mera nadzora i da vlada nije iznela dostupne pravne lekove. Zato je povređen član 8.

8.1.1. Preporuka o policiji

Ustaljeni stav ESLJP-a je da čuvanje i zadržavanje ličnih podataka od policijskih ili tela nacionalne bezbednosti predstavlja mešanje u član 8. stav 1. Evropske konvencije o ljudskim pravima. Mnoge presude ESLJP-a se odnose na obrazloženje takvih mešanja[732].

Primer: U predmetu *B. B. protiv Francuske*[733] podnosilac predstavke je osuđen na zatvorsku kaznu za krivična dela seksualnog zlostavljanja maloletnika u uzrastu od 15 godina kao osoba na položaju od poverenja. Odslužio je zatvorsku kaznu 2000. godine. Posle godinu dana zatražio je da se navod o zatvorskoj kazni ukloni iz njegove krivične evidencije, ali taj zahtev je odbijen. Francuskim zakonom iz 2004. uspostavljena je domaća pravosudna baza podataka seksualnih prestupnika i podnosilac predstavke je obavešten o tome da je uvršten u nju. ESLJP je zaključio da uvrštavanje osuđenog seksualnog prestupnika u domaću pravosudnu bazu podataka potpada pod član 8. Evropske konvencije o ljudskim pravima. Međutim, budući da su uvedene dovoljne mere za zaštitu podataka, kao što je pravo ispitanika da zatraži brisanje podataka, ograničeno trajanje čuvanja podataka i ograničen pristup takvim podacima, postignuta je pravična ravnoteža između sukobljenih privatnih i javnih interesa. ESLJP je zato zaključio da nije došlo do povrede člana 8. Konvencije.

Primer: U predmetu *S. i Marper protiv Ujedinjenog Kraljevstva*[734] oba podnosioca predstavki su optužena, ali ne i osuđena, za krivična dela. Međutim, policija je ipak zadržala i sačuvala njihove otiske prstiju, uzorke ćelija i profile DNK-a. Neograničeno zadržavanje navedenih biometrijskih podataka bilo

732 Videti, na primer, ESLJP, *Leander protiv Švedske*, br. 9248/81, 26. marta 1987; ESLJP, *M. M. protiv Ujedinjenog Kraljevstva*, br. 24029/07, 13. novembra 2012.; ESLJP, *M. K. protiv Francuske*, br. 19522/09, 18. aprila 2013. ili ESLJP, *Aycaguer protiv Francuske*, br. 8806/12, 22. juna 2017.

733 ESLJP, *B. B. protiv Francuske*, br. 5335/06, 17. decembra 2009.

734 ESLJP, *S. i Marper protiv Ujedinjenog Kraljevstva* [VV], br. 30562/04 i 30566/04, 4. decembra 2008, st. 119 i 125.

je dozvoljeno zakonom ako je osoba bila osumnjičena za krivično delo, čak i ako je osumnjičeni kasnije oslobođen optužbi ili pušten na slobodu. ESLJP je smatrao da je sveobuhvatno i neselektivno zadržavanje ličnih podataka koje nije vremenski ograničeno, i pri kojem oslobođeni pojedinci imaju samo ograničene mogućnosti da traže brisanje, predstavljalo nesrazmerno mešanje u prava podnosilaca na poštovanje privatnog života. ESLJP je zato zaključio da je došlo do povrede člana 8. Konvencije.

Ključno pitanje u kontekstu elektronskih komunikacija je mešanje javnih tela u prava na privatnost i zaštitu podataka. Sredstva nadzora ili presretanje komunikacije, poput uređaja za prisluškivanje, dozvoljeni su samo ako je to propisano zakonom i ako predstavlja nužnu meru u demokratskom društvu zbog interesa:

- zaštite državne bezbednosti,
- javne bezbednosti,
- monetarnih interesa države,
- suzbijanja krivičnih dela ili
- zaštite ispitanika ili prava i sloboda drugih osoba.

Mnoge druge presude ESLJP-a odnose se na obrazloženje mešanja u pravo na privatnost vršenjem nadzora.

Primer: U predmetu *Allan protiv Ujedinjenog Kraljevstva*[735] nadležna tela su tajno snimala privatne razgovore zatvorenika sa prijateljem u zatvorskom prostoru za posete i sa saoptuženim u zatvorskoj ćeliji. ESLJP je smatrao da je upotreba uređaja za audio-snimanje i video-snimanje u ćeliji podnosioca predstavke, zatvorskom prostoru za posete i na kolegi zatvoreniku, predstavljala mešanje u njegovo pravo na privatan život. Budući da nije postojao pravni sistem kojim bi se regulisala policijska upotreba tajnih uređaja za snimanje u datom trenutku, navedeno mešanje nije bilo u skladu sa zakonom. ESLJP je stoga zaključio da je došlo do povrede člana 8. Konvencije.

735 ESLJP, *Allan protiv Ujedinjenog Kraljevstva*, br. 48539/99, 5. novembra 2002.

Primer: U predmetu *Roman Zakharov protiv Rusije*[736] podnosilac predstavke je pokrenuo sudski postupak protiv tri operatera mobilnih mreža. Tvrdio je da je prekršeno njegovo pravo na privatnost telefonske komunikacije, jer su operateri postavili opremu koja je omogućila Saveznoj bezbednosnoj službi Ruske Federacije da presretne njegovu telefonsku komunikaciju bez prethodnog sudskog odobrenja. ESLJP je smatrao da domaće zakonske odredbe kojima se uređuje presretanje komunikacija ne pružaju odgovarajuće i delotvorne garancije protiv proizvoljnog postupanja i rizika od zloupotrebe. Naime, domaćim zakonima nije bilo propisano brisanje sačuvanih podataka posle ostvarenja svrhe čuvanja. Zatim, iako je bilo potrebno sudsko odobrenje, sudski nadzor bio je ograničen.

Primer: U predmetu *Szabó i Vissy protiv Mađarske*[737] podnosioci predstavki su tvrdili da se mađarskim zakonodavstvom krši član 8. EKLJP-a, budući da nije bilo dovoljno detaljno niti precizno. Takođe su tvrdili da se zakonodavstvom ne obezbeđuju odgovarajuće garancije protiv zloupotrebe i proizvoljnog postupanja. ESLJP je smatrao da mađarskim zakonima nije propisano da nadzor podleže odobrenju suda. Uprkos tome, ESLJP je napomenuo da, iako je taj nadzor podlegao odobrenju ministra pravosuđa, bio je političke prirode i njime se nije mogla bezbediti potrebna procena „stroge nužnosti". Zatim, domaćim zakonima nije propisano sudsko preispitivanje, budući da se dotičnim osobama ne bi bilo poslato nikakvo obaveštenje. ESLJP je zato zaključio da je došlo do povrede člana 8. Konvencije.

Budući da obrada podataka koju vrše policijske službe može znatno da utiče na lica koja su njom zahvaćena, posebno su potrebna detaljna pravila zaštite podataka prilikom obrade ličnih podataka u toj oblasti. Preporukom o policiji Saveta Evrope nastojalo se da se reši to pitanje davanjem smernica o načinu prikupljanja ličnih podataka za policijske poslove, načinu čuvanja datoteka podataka iz te oblasti, licima koja smeju da pristupe tim datotekama, uključujući uslove za prenos ličnih podataka stranim policijskim telima, načinu na koji ispitanici treba da imaju mogućnost ostvarivanja svojih prava na zaštitu podataka, kao i načinu vršenja kontrole nezavisnih tela. Takođe je razmotrena obaveza pružanja odgovarajuće bezbednosti podataka.

736 ESLJP, *Roman Zakharov protiv Rusije*, br. 47143/06, 4. decembra 2015.

737 ESLJP, *Szabó i Vissy protiv Mađarske*, br. 37138/14, 12. januara 2016.

Preporukom se ne predviđa otvoreno, neselektivno prikupljanje ličnih podataka policijskih organa. Njome se ograničava prikupljanje ličnih podataka koje vrše policijski organi na meru nužnu za sprečavanje stvarne opasnosti ili suzbijanje određenog krivičnog dela. Svako dodatno prikupljanje podataka trebalo bi da se zasniva na posebnom domaćem zakonodavstvu. Obrada osetljivih podataka treba da bude ograničena na meru koja je apsolutno nužna u kontekstu određene istrage.

Ako se lični podaci prikupljaju bez znanja ispitanika, ispitanik se mora obavestiti o prikupljanju podataka čim otkrivanje više ne ometa istragu. Prikupljanje podataka tehničkim nadzorom ili drugim automatizovanim sredstvima takođe se mora zasnivati na posebnoj pravnoj osnovi.

Primer: U predmetu *Versini-Campinchi i Crasnianski protiv Francuske*[738] podnositeljka predstavke, inače advokatica, telefonski je razgovarala s klijentom čija je telefonska linija prisluškivana na zahtev istražnog sudije. Transkript razgovora pokazao je da je ona otkrila informacije obuhvaćene advokatskom tajnom. Tužilac je poslao te informacije Savetu advokatske komore, koji je podnosteljki predstavke izrekla kaznu. ESLJP je potvrdio da je došlo do mešanja u pravo na poštovanje privatnog života i dopisivanja, ne samo lica čiji je telefon prisluškivan, nego i podnositeljke predstavke čija je komunikacija presretana i transkribovana. Mešanje je izvršeno u skladu sa zakonom i imalo je legitiman cilj sprečavanja narušavanja reda. Podnositeljka predstavke je izdejstvovala preispitivanje zakonitosti podnošenja transkripta prisluškivanog telefonskog razgovora u kontekstu disciplinskog postupka koji se vodio protiv nje. Iako nije mogla da podnese zahtev za poništavanje transkripta telefonskog razgovora, ESLJP je smatrao da je postojao delotvoran nadzor kojim se sporno mešanje moglo ograničiti na ono što je nužno u demokratskom društvu. ESLJP je smatrao neuverljivim argument da mogućnost krivičnog postupka protiv advokata na osnovu transkripta može imati negativan efekat na slobodu komunikacije između advokata i njegovog klijenta, a stoga i na prava na odbranu tog klijenta, kada advokatsko otkrivanje informacija može predstavljati protivzakonito postupanje s njene strane. Stoga nije došlo do povrede člana 8.

U Preporuci o policiji Saveta Evrope naveden je zaključak da se pri čuvanju ličnih podataka moraju jasno razlikovati administrativni podaci od policijskih podataka, lični podaci različitih vrsta ispitanika, kao što su osumnjičeni, osuđenici, žrtve i sve-

738 ESLJP, *Versini-Campinchi i Crasnianski protiv Francuske*, br. 49176/11, 16. juna 2016.

doci, kao i podaci koji se smatraju čvrstim činjenicama od onih koji se zasnivaju na sumnjama ili nagađanjima.

Svrha u koju se policijski podaci mogu upotrebiti mora biti strogo ograničena. To ima posledice na otkrivanje policijskih podataka trećim stranama. Prenos ili otkrivanje takvih podataka unutar policijskog sektora treba da zavisi od toga da li postoji legitiman interes za deljenje informacija. Prenos ili otkrivanje takvih podataka izvan policijskog sektora treba da bude dozvoljeno samo ako postoji jasna pravna obaveza ili ovlašćenje.

Primer: U predmetu *Karabeyoğlu protiv Turske*[739] telefonske linije tužioca, inače sudije, praćene su u okviru krivične istrage nezakonite organizacije čiji je on navodno bio član ili kojoj je navodno pružao pomoć i podršku. Nakon donošenja odluke da neće pokrenuti krivični postupak, javni tužilac zadužen za krivičnu istragu uništio je predmetne snimke. Međutim, primerak je ostao u posedu sudskih istražitelja koji su te materijale iskoristili u kontekstu disciplinske istrage protiv podnosiocaa predstavke. ESLJP je smatrao da je prekršeno merodavno zakonodavstvo jer su informacije upotrebljene u svrhe u koje nisu prikupljene i nisu uništene unutar zakonskog roka. Mešanje u pravo na poštovanje privatnog života podnosioca predstavke nije bilo u skladu sa zakonom kad je bila reč o disciplinskom postupku pokrenutom protiv njega.

Međunarodni prenos ili otkrivanje podataka treba da bude ograničeno prema stranim policijskim organima i da se zasniva na posebnim zakonskim odredbama, možda i međunarodnim sporazumima, osim ako je to nužno za sprečavanje ozbiljne i neposredne opasnosti.

Obrada podataka koju vrši policija mora da bude podvrgnuta nezavisnom nadzoru kako bi se obezbedila usklađenost sa nacionalnim zakonodavstvom o zaštiti podataka. Ispitanici moraju da imaju sva prava na pristup utvrđena u modernizovanoj Konvenciji br. 108. Kada su prava ispitanika na pristup ograničena na osnovu člana 9. Konvencije br. 108, u interesu delotvornih policijskih istraga i izvršavanja krivičnopravnih sankcija, ispitanici moraju imati pravo žalbe domaćem nadzornom telu za zaštitu podataka ili drugom nezavisnom telu u skladu sa domaćim zakonom.

739 ESLJP, *Karabeyoğlu protiv Turske*, br. 30083/10, 7. juna 2016.

8.1.2. Budimpeštanska konvencija o kibernetičkom kriminalu

Budući da se u kriminalnim aktivnostima sve češće koriste elektronski sistemi za obradu podataka, i one na njih utiču, potrebne su nove krivičnopravne odredbe kojima se rešava taj problem. Stoga je Savet Evrope doneo međunarodni pravni instrument, Konvenciju o kibernetičkom kriminalu, poznatu i kao Budimpeštanska konvencija, kao odgovor na problem krivičnih dela učinjenih nad elektronskim mrežama i putem njih.[740]

Toj Konvenciji mogu pristupiti i države koje nisu članice Saveta Evrope. Do početka 2018. godine 14 država izvan Saveta Evrope[741] pristupilo je Konvenciji, a sedam drugih nečlanica pozvano je da se pridruži.

Konvencija o kibernetičkm kriminalu i dalje je najuticajniji međunarodni sporazum koji se bavi kršenjima zakona putem interneta ili drugih informatičkih mreža. Njene strane moraju ažurirati i uskladiti svoje krivične zakone protiv hakovanja i ostalih povreda bezbednosti, uključujući povrede autorskih prava, računarski potpomognutu prevaru, dečju pornografiju i druge zabranjene kibernetičke aktivnosti. Konvencijom su propisana i procesna ovlašćenja koja obuhvataju pretraživanje računarskih mreža i presretanje komunikacija u kontekstu suzbijanja kibernetičkog kriminala. Konačno, njome je omogućena delotvorna međunarodna saradnja. Dodatni protokol uz Konvenciju odnosi se na kriminalizaciju rasističke i ksenofobične propagande na računarskim mrežama.

Iako Konvencija zapravo nije instrument za unapređenje zaštite podataka, njome se kriminalizuju aktivnosti za koje je verovatno da će povrediti prava ispitanika na zaštitu njegovih podataka. U skladu sa Konvencijom, ugovorne strane moraju doneti zakonodavne mere kojima će omogućiti domaćim telima da presretnu podatke o potrošnji i sadržaju[742]. Njome se ugovorne strane takođe obavezuju da pri sprovođenju Konvencije predvide odgovarajuću zaštitu ljudskih prava i sloboda, uključujući

740 Savet Evrope, Komitet ministara (2001), Konvencija o visokotehnološkom kriminalu, CETS br. 185, Budimpešta, 23. novembra 2001, stupila na snagu 1. jula 2004.

741 Australija, Kanada, Čile, Kolumbija, Dominikanska Republika, Izrael, Japan, Mauricijus, Panama, Senegal, Šri Lanka, Tonga, Tunis i Sjedinjene Američke Države. Pogledajte Tablicu s potpisima i datumima ratifikacije Sporazuma br. 185, status u srpnju 2017. (dostupno na engleskom jeziku).

742 Savet Europe, Komitet ministara (2001.), Konvencija o kibernetičkom kriminalu, CETS br. 185, Budimpešta, 23. novembra 2001., članovi 20. i 21.

prava garantovana EKLJP-om, kao što je pravo na zaštitu podataka[743]. Ugovorne strane ne moraju potpisati Konvenciju br. 108 da bi pristupile Budimpeštanskoj konvenciji o visokotehnološkom kriminalu.

8.2. Pravo zaštite podataka EU u oblasti policije i krivičnog pravosuđa

Ključne tačke

- U okviru Evropske unije, zaštita podataka u policijskom i krivičnopravnom sektoru uređena je u kontekstu domaće i prekogranične obrade koju vrše policija i tela krivičnog pravosuđa država članica i nadležna tela EU.
- Na nivou država članica Direktiva o zaštiti podataka za policiju i tela krivičnog pravosuđa mora se ugraditi u domaće pravo.
- Posebnim pravnim instrumentima uređuje se zaštita podataka u prekograničnoj saradnji policije i drugih organa reda, naročito u oblasti borbe protiv terorizma i prekograničnog kriminala.
- Postoje posebni propisi za zaštitu podataka za Evropsku policijsku službu (Europol), Agenciju Evropske unije za saradnju u krivičnom pravosuđu (Eurojust) kao i novoosnovanu Kancelariju evropskog javnog tužioca, koji su svi tela EU koja pomažu i unapređuju prekogranično sprovođenje prava.
- Posebni propisi za zaštitu podataka postoje i za zajedničke informacione sisteme uspostavljene na nivou Evropske unije za prekograničnu razmenu informacija između nadležnih policijskih i pravosudnih tela. Važni su primeri Šengenski informacioni sistem II (ŠIS II), Vizni informacioni sistem (VIS) i Eurodac, centralizovani sistem sa podacima o otiscima prstiju državljana trećih zemalja i lica bez državljanstva koja su podnela zahtev za azil u jednoj od država članica EU.
- U toku je postupak ažuriranja navedenih odredbi o zaštiti podataka u EU, kako bi bile u skladu s odredbama Direktive o zaštiti podataka za policiju i tela krivičnog pravosuđa.

8.2.1. Direktiva o zaštiti podataka za policiju i tela krivičnog pravosuđa

Direktivom 2016/680/EU o zaštiti pojedinaca u vezi s obradom ličnih podataka od strane nadležnih tela u svrhe sprečavanja, istrage, otkrivanja ili gonjenja krivič-

743 *Ibid.*, član 15. stav 1.

nih dela ili izvršavanja krivičnih sankcija i o slobodnom kretanju takvih podataka (Direktiva o zaštiti podataka za policiju i tela krivičnog pravosuđa)[744] nastoji se da se zaštite lični podaci koji su prikupljeni i obrađeni u svrhe krivičnog prava, na primer:

- sprečavanja, istrage, otkrivanja ili gonjenja krivičnih dela ili izvršavanja krivičnih sankcija, uključujući zaštitu od pretnji javnoj bezbednosti i njihovo sprečavanje,
- izvršavanja krivične sankcije i
- u slučajevima kada policija ili drugi organi reda nastoje da obezbede poštovanje zakona i zaštitu od pretnji javnoj bezbednosti i osnovnim pravima društva koje mogu da predstavljaju krivično delo i da spreče takve pretnje.

Direktivom o zaštiti podataka za policiju i tela krivičnog prava štite se lični podaci različitih kategorija pojedinaca koji učestvuju u krivičnim postupcima, poput svedoka, doušnika, žrtvi, osumnjičenih i saučesnika. Policija i tela krivičnog pravosuđa dužni su da poštuju odredbe Direktive kad god obrađuju takve lične podatke u svrhu rada organa reda, a u okviru personalne i stvarne oblasti primene Direktive[745].

Međutim, u određenim uslovima dozvoljena je i upotreba podataka u druge svrhe. Obrada podataka u svrhu sprovođenja prava, koja se razlikuje od one u koju su izvorno prikupljeni, dozvoljena je samo ako je to zakonito, nužno i srazmerno na osnovu domaćeg prava ili prava Unije[746]. Na te druge svrhe primenjuju se odredbe Opšte uredbe o zaštiti podataka. Beleženje i dokumentovanje deljenja podataka je jedna od posebnih dužnosti nadležnih tela radi pomaganja u pojašnjenju odgovornosti koje proizlaze iz prigovora.

Nadležna tela koja deluju u oblasti rada policije i krivičnog pravosuđa su javna tela ili tela koja su ovlašćena na osnovu domaćeg zakonodavstva i javnih ovlašćenja za

744 Direktiva 2016/680/EU Evropskog parlamenta i Saveta od 27. aprila 2016. o zaštiti pojedinaca u vezi s obradom ličnih podataka od strane nadležnih tela u svrhe sprečavanja, istrage, otkrivanja ili gonjenja krivičnih dela ili izvršavanja krivičnih sankcija i o slobodnom kretanju takvih podataka kao i o stavljanju van snage Okvirne odluke Saveta 2008/977/PUP, SL 2016 L 119, str. 89. (Direktiva o zaštiti podataka za policiju i tela krivičnog pravosuđa).

745 Direktiva o zaštiti podataka za policiju i tela krivičnog pravosuđa, član 2. stav 1.

746 *Ibid*., član 4. stav 2.

obavljanje funkcija javnih tela[747], npr. privatni zatvori[748]. Oblast primene Direktive obuhvata obradu podataka na domaćem nivou i prekograničnu obradu između policijskih i pravosudnih tela država članica, kao i međunarodne prenose koje nadležna tela vrše prema trećim zemljama i međunarodnim organizacijama[749]. Ona ne obuhvata nacionalnu bezbednost niti obradu ličnih podataka koju vrše institucije, tela, kancelarije i agencije EU[750].

Direktiva se u velikoj meri zasniva na načelima i definicijama iz Opšte uredbe o zaštiti podataka, uzimajući u obzir posebnu prirodu oblasti policije i krivičnog pravosuđa. Nadzor mogu da vrše ista nadležna tela države članice koja ga vrše i na osnovu Opšte uredbe o zaštiti podataka. Imenovanje službenika za zaštitu podataka i vršenje procena efekata zaštite podataka uvedeni su u Direktivu kao nove obaveze za policijska i tela krivičnog pravosuđa[751]. Iako su ti koncepti nadahnuti Opštom uredbom o zaštiti podataka, Direktiva se odnosi na posebnu prirodu policijskih tela i tela krivičnog pravosuđa. U poređenju s obradom podataka u komercijalne svrhe, koja je regulisana Uredbom, za obradu u vezi sa bezbednošću može biti potreban određeni nivo fleksibilnosti. Na primer, obezbeđenje jednakog nivoa zaštite ispitanika u pogledu prava na informacije i pristup sopstvenim ličnim podacima ili njihovo brisanje, kao što je omogućena Opštom uredbom o zaštiti podataka, moglo bi podrazumevati da bi svaka radnja nadzora koja se vrši u svrhe zavođenja reda postala nedelotvorna u kontekstu sprovođenja. Direktiva stoga ne sadrži načelo transparentnosti. Na sličan način se i načela smanjenja količine podataka i ograničenja svrhe, prema kojima se lični podaci moraju ograničiti na ono što je nužno za svrhe u koje se obrađuju, te obrađivati u utvrđene i izričite svrhe, moraju fleksibilno primenjivati u sklopu obrade u bezbednosne svrhe. Podaci koje prikupe i čuvaju nadležna tela u određenom predmetu mogu se pokazati izuzetno korisnima u rešavanju budućih predmeta.

747 *Ibid.*, član 3. stav 7.

748 Evropska komisija (2016), Komunikacija Komisije Evropskom parlamentu na osnovu člana 294. stav 6. Ugovora o funkcionisanju Evropske unije o stavu Saveta o donošenju Direktive Evropskog parlamenta i Saveta o zaštiti pojedinaca pri obradi ličnih podataka od strane nadležnih tela u svrhe sprečavanja, istrage, otkrivanja ili gonjenja krivičnih dela ili izvršavanja krivičnopravnih sankcija kao i slobodnom kretanju takvih podataka i o stavljanju van snage Okvirne odluke Saveta 2008/977/PUP, COM(2016) 213 final, Bruxelles, 11. aprila 2016.

749 Direktiva o zaštiti podataka za policiju i tela krivičnog pravosuđa, poglavlje V.

750 *Ibid.*, član 2. stav 3.

751 *Ibid.*, član 32. odnosno član 27.

Načela u vezi s obradom

U Direktivi o zaštiti podataka za policiju i tela krivičnog pravosuđa utvrđuju se određene ključne zaštitne mere u vezi s upotrebom ličnih podataka. Takođe se navode načela na kojima se zasniva obrada tih podataka. Države članice moraju da obezbede da su lični podaci:

- obrađivani zakonito i pravično,
- prikupljeni u posebne, izričite i zakonite svrhe i da se ne obrađuju na način koji nije u skladu s tim svrhama,
- primereni i relevantni i da nisu preterani u odnosu na svrhe u koje se obrađuju,
- tačni i prema potrebi ažurirani; mora se preduzeti svaka razumna mera radi obezbeđenja da se lični podaci koji nisu tačni, uzimajući u obzir svrhe u koje se obrađuju, bez odlaganja izbrišu ili isprave,
- čuvani u obliku koji omogućava identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe u koje se lični podaci obrađuju,
- obrađivani na način kojim se obezbeđuje odgovarajuća sigurnost ličnih podataka, uključujući zaštitu od neovlašćene ili nezakonite obrade kao i od slučajnog gubitka, uništenja ili oštećenja primenom odgovarajućih tehničkih ili organizacionih mera[752].

U skladu sa Direktivom, obrada je zakonita samo u onoj meri u kojoj je nužna kako bi se obavili pojedini zadaci. Usto, to bi trebalo da vrši nadležno telo u svrhu ostvarenja ciljeva navedenih u Direktivi i tako da bi trebalo da se zasniva na pravu Unije ili domaćem pravu[753]. Podaci se ne smeju čuvati duže nego što je potrebno i moraju se izbrisati ili povremeno pregledati unutar određenih vremenskih okvira. Sme ih upotrebljavati isključivo nadležno telo, i to u svrhu u koju su oni prikupljeni, preneseni ili stavljeni na raspolaganje.

752 *Ibid.*, član 4. stav 1.

753 *Ibid.*, član 8.

Prava ispitanika

Direktivom se takođe utvrđuju prava ispitanika. Ona uključuju sledeće:

- pravo na informacije. Države članice moraju propisati obavezu rukovaocu podacima da ispitaniku na raspolaganje stavi: 1) identitet i kontakt podatke rukovaoca podacima, 2) kontakt podatke službenika za zaštitu podataka, 3) svrhe predviđene obrade, 4) pravo na podnošenje prigovora nadzornom telu i kontakt podatke nadzornog tela kao i 5) pravo na pristup ličnim podacima, njihovu ispravku ili brisanje, ili ograničavanje obrade podataka[754]. Uz te opšte zahteve za informacije, Direktivom se utvrđuje da u određenim slučajevima, kako bi se ispitanicima omogućilo ostvarivanje njihovih prava, rukovaoci podacima moraju da daju informacije o pravnoj osnovi obrade i o periodu čuvanja podataka. Ako će se lični podaci prenositi drugim primaocima, uključujući treće zemlje ili međunarodne organizacije, ispitanici moraju da budu obavešteni o kategorijama takvih primalaca. Konačno, rukovaoci podacima moraju da daju sve dodatne informacije, uzimajući u obzir posebne okolnosti u kojima se podaci obrađuju, na primer slučajeve prikupljanja ličnih podataka u sklopu tajnog nadzora, odnosno bez znanja ispitanika. Time se garantuje pravična obrada za ispitanika[755],

- pravo na pristup ličnim podacima. Države članice moraju da obezbede da ispitanik uživa pravo da zna da li se njegovi lični podaci obrađuju. Ako se oni obrađuju, ispitanik treba da ima pristup određenim informacijama, kao što su kategorije podataka koji se obrađuju[756]. Međutim, to pravo se može ograničiti, na primer kako bi se izbeglo ometanje istrage ili dovođenje u pitanje gonjenja krivičnih dela ili kako bi se zaštitila javna bezbednost kao i prava i slobode drugih[757],

- pravo na ispravku ličnih podataka. Države članice dužne su da obezbede da ispitanik bez nepotrebnog odlaganja može da dobije ispravku netačnih ličnih podataka. Zatim, ispitanik takođe ima pravo da dopuni nepotpune lične podatke[758],

- pravo na brisanje ličnih podataka i ograničavanje obrade. U određenim slučajevima rukovalac podacima mora izbrisati lične podatke. Zatim, ispitanik može

754 *Ibid.*, član 13. stav 1.
755 *Ibid.*, član 13. stav 2.
756 *Ibid.*, član 14.
757 *Ibid.*, član 15.
758 *Ibid.*, član 16. stav 1.

da obezbedi brisanje svojih ličnih podataka, ali samo kada se oni nezakonito obrađuju[759]. U određenim situacijama može se ograničiti obrada ličnih podataka umesto brisanja podataka. To se može desiti 1) kada se osporava tačnost ličnih podataka, ali se to ne može sa sigurnošću utvrditi ili 2) kada su lični podaci potrebni kao dokaz[760].

Kad god rukovalac podacima odbije da ispravi ili izbriše lične podatke ili ograniči obradu podataka, ispitanik se o tome mora obavestiti pisanim putem. Države članice mogu to pravo na informacije da ograniče radi, između ostalog, zaštite javne bezbednosti ili prava i sloboda drugih, iz istih razloga kao i kada se ograničava pravo na pristup[761].

Ispitanik obično ima pravo na informacije o obradi svojih ličnih podataka i ima pravo na pristup, ispravku ili brisanje podataka ili pak ograničavanje njihove obrade, koje može da ostvari direktno putem rukovaoca podacima. Druga mogućnost, posredno ostvarivanje prava ispitanika putem nadzornog tela za zaštitu podataka, dopuštena je na osnovu Direktive o zaštiti podataka za policiju i tela krivičnog pravosuđa, a počinje da važi kada rukovalac podacima ograniči prava ispitanika[762]. Članom 17. Direktive propisuje se da države članice donose mere kojima se obezbeđuje da se prava ispitanika mogu ostvariti i putem nadležnog nadzornog tela. Zbog toga rukovalac podacima mora da obavesti ispitanika o mogućnosti posrednog pristupa.

Obaveze rukovaoca podacima i obrađivača podataka

U kontekstu Direktive o zaštiti podataka za policiju i tela krivičnog pravosuđa rukovaoci podacima su nadležna javna tela ili druga tela s odgovarajućim javnim ovlašćenjima i javnim vlastima, koja utvrđuju svrhe i načine obrade ličnih podataka. Direktivom se utvrđuje nekoliko obaveza rukovaoca podacima kako bi se obezbedio visok nivo zaštite ličnih podataka koji se obrađuju u svrhe održavanja javnog reda i mira.

Nadležna tela moraju da vode beleške/evidenciju o postupcima obrade koje vrše putem automatizovanih sistema obrade. Zapisi se moraju beležiti barem za prikupljanje, izmene, obavljanje uvida, otkrivanje, uključujući prenose, kombinovanje i

759 *Ibid.*, član 16. stav 2.

760 *Ibid.*, član 16. stav 3.

761 *Ibid.*, član 16. stav 4.

762 *Ibid.*, član 17.

brisanje ličnih podataka[763]. Direktivom se, takođe, utvrđuje da zapisi o obavljanju uvida i otkrivanju moraju omogućiti da se ustanovi datum i vreme takvih postupaka, njihovo obrazloženje, kao i, ako je to moguće, identitet osobe koja je obavila uvid ili otkrila lične podatke i identitet primaoca takvih ličnih podataka. Zapisi se moraju upotrebljavati samo u svrhe provere zakonitosti obrade, samopraćenja i obezbeđenja celovitosti i bezbednosti ličnih podataka i za krivične postupke[764]. Na zahtev nadzornog tela rukovalac podacima i obrađivač podataka moraju mu staviti zapise na raspolaganje.

Posebno je propisana opšta obaveza da rukovaoci podacima izvrše odgovarajuće tehničke i organizacione mere kako bi obezbedili da se obrada vrši u skladu s Direktivom i kako bi mogli da dokažu zakonitost takve obrade[765]. Prilikom uspostavljanja takvih mera, oni moraju uzeti u obzir prirodu, opseg i kontekst obrade, kao i posebno moguće rizike za prava i slobode pojedinaca. Rukovaoci podacima treba da donesu interna pravila i sprovedu mere koje olakšavaju usklađenost sa načelima zaštite podataka, a naročito načelom tehničke i integrisane zaštite podataka[766]. Ako je verovatno da će obrada prouzrokovati visok rizik za prava pojedinaca, na primer zbog primene novih tehnologija, rukovaoci podacima moraju izvršiti procenu efekta zaštite podataka pre obrade[767]. U Direktivi se takođe navode mere koje rukovaoci podacima moraju sprovesti kako bi obezbedili sigurnost obrade. One uključuju mere sprečavanja neovlašćenog pristupa ličnim podacima koje oni obrađuju, obezbeđivanja da ovlašćene osobe imaju pristup samo ličnim podacima koji su obuhvaćeni njihovim ovlašćenjem za pristup, da funkcije sistema obrade ispravno rade i da se sačuvani lični podaci ne mogu ugroziti zbog nedostataka u funkcionisanju sistema[768]. Ako ipak dođe do povrede ličnih podataka, rukovaoci podacima moraju da obaveste nadzorno telo u roku od tri dana, navodeći prirodu povrede, njene verovatne posledice, kategorije zahvaćenih ličnih podataka i približan broj dotičnih ispitanika. O povredi ličnih podataka mora se obavestiti i ispitanik, „bez nepotrebnog odlaganja", ako je verovatno da će povreda prouzrokovati visok rizik za njegova prava i slobode[769].

763 *Ibid.*, član 25. stav 1.
764 *Ibid.*, član 25. stav 2.
765 *Ibid.*, član 19.
766 *Ibid.*, član 20.
767 *Ibid.*, član 27.
768 *Ibid.*, član 29.
769 *Ibid.*, članovi 30. i 31.

Direktiva sadrži načelo odgovornosti, prema kojem rukovaoci podacima imaju dužnost da sprovedu mere kojima će obezbediti usklađenost s tim načelom. Rukovaoci podacima moraju voditi evidenciju o svim kategorijama aktivnosti obrade za koje su nadležni: detaljan sadržaj te evidencije utvrđen je u članu 24. Direktive. Evidencija se po zahtevu mora staviti na raspolaganje nadzornom telu kako bi ono moglo da nadgleda postupke obrade rukovalaca podacima. Druga važna mera za povećanje odgovornosti je imenovanje službenika za zaštitu podataka (SZP). Rukovaoci podacima moraju imenovati službenika za zaštitu podataka, iako se Direktivom omogućava da države članice izuzmu sudove i druga nezavisna pravosudna tela od te obaveze[770]. Dužnosti SZP-a slične su onima koje su utvrđene Opštom uredbom o zaštiti podataka. Službenik za zaštitu podataka nadgleda usklađenost sa Direktivom, daje informacije i savetuje zaposlene koji vrše obradu podataka o njihovim obavezama prema zakonodavstvu o zaštiti podataka. SZP takođe daje savete o potrebi vršenja procene efekta zaštite podataka i deluje kao kontakt tačka nadzornog tela.

Prenosi trećim zemljama ili međunarodnim organizacijama

Slično kao i Opštom uredbom o zaštiti podataka, Direktivom se utvrđuju uslovi prenosa ličnih podataka u treće zemlje ili međunarodne organizacije. Kad bi se lični podaci slobodno prenosili izvan nadležnosti EU, mogle bi se narušiti zaštitne mere i snažna zaštita obezbeđeni pravom EU. Međutim, sami uslovi znatno se razlikuju od onih iz Opšte uredbe o zaštiti podataka. Prenos ličnih podataka u treće zemlje ili međunarodne organizacije dozvoljen je[771]:

- ako je prenos nužan za ciljeve Direktive,
- ako se lični podaci prenose nadležnom telu treće zemlje ili međunarodne organizacije u smislu Direktive, iako su moguća odstupanja od tog pravila u pojedinačnim i posebnim slučajevima[772],
- ako je za prenos ličnih podataka primljenih u okviru prekogranične saradnje trećim zemljama ili međunarodnim organizacijama potrebno odobrenje države članice iz koje podaci potiču, ali postoje izuzeci u hitnim slučajevima,

770 *Ibid.*, član 32.

771 *Ibid.*, član 35.

772 *Ibid.*, član 39.

- ako je Evropska komisija donela odluku o primerenosti, ako su uspostavljene odgovarajuće zaštitne mere ili se primenjuje odstupanje za prenose u posebnim situacijama,

- ako je za dalje prenose ličnih podataka trećoj zemlji ili međunarodnoj organizaciji potrebno prethodno odobrenje nadležnog tela koje je izvršilo prvobitni prenos za koje će se, između ostalog, uzeti u obzir ozbiljnost krivičnog dela i nivo zaštite podataka u odredišnoj zemlji drugog međunarodnog prenosa podataka[773].

U skladu sa Direktivom, prenosi ličnih podataka mogu da se odvijaju ako je ispunjen jedan od tri uslova. Prvi se odnosi na slučaj u kojem je Evropska komisija donela odluku o primerenosti na osnovu Direktive. Odluka se može primenjivati na celu državnu oblast ili određene sektore treće zemlje ili međunarodne organizacije. Međutim, to je moguće samo ako se obezbedi odgovarajuć nivo zaštite i ako su ispunjeni uslovi iz Direktive[774]. U takvim slučajevima prenosi ličnih podataka ne podležu odobrenju države članice[775]. Evropska komisija mora pratiti razvoj događaja koji bi mogli da utiču na efikasnost odluka o primerenosti. Osim toga, odluka mora sadržati mehanizam za periodično preispitivanje. Komisija takođe može staviti van snage, izmeniti ili suspendovati odluku ako dostupne informacije upućuju na to da uslovi u trećoj zemlji ili međunarodnoj organizaciji više ne obezbeđuju odgovarajući nivo zaštite. U tom slučaju Komisija mora da započne savetovanje s trećom zemljom ili međunarodnom organizacijom radi popravljanja stanja.

Ako ne postoji odluka o primerenosti, prenosi se mogu zasnivati na odgovarajućim zaštitnim merama. One mogu biti utvrđene pravno obavezujućim instrumentom ili rukovalac podacima može izvršiti samoprocenu okolnosti prenosa ličnih podataka i zaključiti da postoje odgovarajuće zaštitne mere. Prilikom samoprocene trebalo bi da se uzmu u obzir mogući sporazumi o saradnji zaključeni između Europol-a ili Eurojust-a i treće zemlje ili međunarodne organizacije, postojanje obaveza poverljivosti i ograničenja svrhe, kao i garancije da se podaci neće upotrebljavati ni za koji oblik okrutnog i nečovečnog postupanja, uključujući izvršenje smrtne kazne[776]. U potonjem slučaju rukovalac podacima mora da obavesti nadležno nadzorno telo o kategorijama prenosa na osnovu ove kategorije[777].

773 *Ibid.*, član 35. stav 1.

774 *Ibid.*, član 36.

775 *Ibid.*, član 36. stav 1.

776 *Ibid.*, uvodna izjava 71.

777 *Ibid.*, član 37. stav 1.

Čak i ako nije donesena odluka o primerenosti ili nisu uspostavljene odgovarajuće zaštitne mere, prenosi se i dalje mogu dozvoliti u posebnim situacijama navedenim u Direktivi. One, između ostalog, uključuju zaštitu vitalnih interesa ispitanika ili druge osobe kao i sprečavanje neposredne i ozbiljne pretnje javnoj bezbednosti države članice ili treće zemlje[778].

U pojedinim i posebnim slučajevima prenosi nadležnih tela primaocima sa boravištem u trećim zemljama koji nisu nadležna tela mogu se vršiti ako su uz jedan od tri uslova koji su opisani iznad ispunjeni i dodatni uslovi utvrđeni u članu 39. Direktive. Tačnije, prenos mora biti strogo nužan za obavljanje zadatka nadležnog tela koje vrši prenos, koje je takođe odgovorno za potvrdu da nikakva osnovna prava ili slobode pojedinaca nemaju prednost pred javnim interesom kojim se opravdava prenos. Takvi prenosi se moraju dokumentovati, a nadležno telo koje vrši prenos mora obavestiti nadležno nadzorno telo[779].

Kad je reč o trećim zemljama i međunarodnim organizacijama, Direktivom se takođe nalaže razvoj mehanizama međunarodne saradnje za olakšavanje delotvornog izvršavanja zakonodavstva i pomaganje nadzornim telima za zaštitu podataka da sarađuju sa sličnim telima u drugim zemljama[780].

Nezavisni nadzor i pravni lekovi za ispitanike

Svaka država članica mora da obezbedi da jedno ili više nezavisnih domaćih nadzornih tela bude odgovorno za savetovanje i nadzor primene odredbi usvojenih u skladu s Direktivom[781]. Nadzorno telo uspostavljeno za potrebe Direktive može biti isto kao nadzorno telo uspostavljeno na osnovu Opšte uredbe o zaštiti podataka, ali države članice imaju slobodu imenovanja drugog tela, pod uslovom da ono ispunjava kriterijume nezavisnosti. Nadzorna tela moraju takođe da saslušaju zahteve koje podnese bilo koje lice u vezi sa zaštitom njegovih prava i sloboda u pogledu obrade ličnih podataka koju vrše nadležna tela.

Ako je ostvarenje prava ispitanika odbijeno iz opravdanih razloga, ispitanik mora imati pravo na žalbu nadležnom domaćem nadzornom telu i/ili sudu. Ako osoba pretrpi štetu zbog nepoštovanja domaćeg zakonodavstva kojim se sprovodi Direk-

778 *Ibid.*, član 38. stav 1.

779 *Ibid.*, član 37. stav 3.

780 *Ibid.*, član 40.

781 *Ibid.*, član 41.

tiva, ima pravo na naknadu od rukovaoca podacima ili bilo kojeg drugog tela nadležnog na osnovu zakonodavstva države članice[782]. Uopšte, ispitanici moraju imati na raspolaganju pravni lek u slučaju bilo kog kršenja prava koja su im garantovana domaćim zakonodavstvom kojim se sprovodi Direktiva[783].

8.3. Ostali specifični pravni instrumenti za zaštitu podataka u pitanjima održavanja javnog reda i mira

Osim Direktivom o zaštiti podataka za policiju i tela krivičnog pravosuđa, razmena informacija koje države članice poseduju u posebnim oblastima uređena je nizom pravnih instrumenata, kao što su: Okvirna odluka Saveta 2009/315/PUP o organizaciji i sadržaju razmene podataka iz krivične evidencije između država članica, Odluka Saveta 2000/642/PUP o uređenju saradnje između finansijsko-obaveštajnih jedinica država članica u vezi sa razmenom informacija i Okvirna odluka Saveta 2006/960/PUP od 18. decembra 2006. o pojednostavljenju razmene informacija i obaveštajnih podataka između tela zaduženih za održavanje javnog reda i mir u državama članicama Evropske unije[784].

Važno je napomenuti da prekogranična saradnja[785] nadležnih tela sve više uključuje razmenu imigracionih podataka. Ta oblast prava ne smatra se delom policijskih i krivičnopravnih pitanja, ali u mnogočemu je relevantna za rad policije i pravosudnih tela. Isto važi za podatke o robi koja se uvozi u Evropsku uniju ili izvozi iz nje. Ukidanjem unutarnjih graničnih kontrola u šengenskom prostoru povećan je rizik od prevare, pa države članice moraju pojačati saradnju, naročito poboljšanjem prekogranične razmene podataka radi delotvornijeg otkrivanja i krivičnog gonjenja zbog kršenja domaćeg carinskog prava i carinskog prava Evropske unije. Usto, u prote-

782 *Ibid.*, član 56.

783 *Ibid.*, član 54.

784 Savet Evropske unije (2009), Okvirna odluka Saveta 2009/315/PUP od 26. februara 2009. o organizaciji i sadržaju razmene podataka iz kaznene evidencije između država članica, SL 2009 L 93; Savet Evropske unije (2000.), Odluka Saveta 2000/642/PUP od 17. oktobra 2000. o uređenju saradnje između finansijsko-obaveštajnih jedinica država članica u vezi sa razmenom informacija, SL 2000 L 271; Okvirna odluka Saveta 2006/960/PUP od 18. decembra 2006. o pojednostavljenju razmene informacija i obaveštajnih podataka između tela zaduženih za izvršavanje zakona u državama članicama Evropske unije, SL L 386.

785 Evropska komisija (2012.), Komunikacija Komisije Evropskom parlamentu i Savetu, „Jačanje pravosudne saradnje u Evropskoj uniji: Evropski model za razmenu informacija (EIXM)", COM(2012) 735 final, Bruxelles, 7. decembra 2012.

klih nekoliko godina vidljiv je porast teškog i organizovanog kriminala i terorizma, koji mogu uključivati međunarodna putovanja, pa je u mnogim slučajevima uočena potreba za povećanom prekograničnom saradnjom policije i tela nadležnih za održavanje javnog reda i mira[786].

Prumska odluka

Važan primer institucionalizacije prekogranične saradnje razmenom podataka koji se čuvaju na domaćem nivou jeste Odluka Saveta 2008/615/PUP, zajedno s odredbama za sprovođenje iz Odluke 2008/616/PUP, o produbljivanju prekogranične saradnje, posebno u suzbijanju terorizma i prekograničnog kriminala (Prumska odluka), kojom je Prumski ugovor ugrađen u pravo EU 2008.[787] Prumski ugovor je ugovor o međunarodnoj policijskoj saradnji koji su 2005. potpisali Austrija, Belgija, Francuska, Nemačka, Luksemburg, Holandija i Španija[788].

Cilj Prumske odluke je da se pomogne državama ugovornicama u poboljšanju razmene informacija radi sprečavanja i suzbijanja kriminala u tri oblasti: terorizmu, prekograničnom kriminalu i nezakonitoj migraciji. U tu svrhu se u odluci navode odredbe u pogledu:

- automatizovanog pristupa DNK profilima, podacima o otiscima prstiju i određenim domaćim podacima o registraciji vozila,
- dostave podataka u vezi s važnim događajima prekogranične prirode,
- dostave informacija radi sprečavanja terorističkih krivičnih dela,
- drugih mera za produbljivanje prekogranične policijske saradnje.

Za baze podataka koje se stavljaju na raspolaganje prema Prumskoj odluci u potpunosti je nadležno domaće zakonodavstvo, ali razmena podataka dodatno je ure-

786 Vidi Evropska komisija (2011), Predlog direktive Evropskog parlamenta i Saveta o upotrebi podataka iz evidencije podataka o putnicima (PNR) u svrhu sprečavanja, otkrivanja, istrage i krivičnog gonjenja krivičnih dela terorizma i teških krivičnih dela, COM(2011) 32 final, Bruxelles, 2. februara 2011, str. 1.

787 Savet Evropske unije (2008.), Odluka Saveta 2008/615/PUP od 23. juna 2008. o produbljivanju prekogranične saradnje, posebno u suzbijanju terorizma i prekograničnog kriminala, SL 2008 L 210.

788 Konvencija (dostupna na engleskom jeziku) između Kraljevine Belgije, Savezne Republike Nemačke, Kraljevine Španije, Francuske Republike, Velikog Vojvodstva Luksemburga, Kraljevine Holandije i Republike Austrije o produbljivanju prekogranične saradnje, posebno u suzbijanju terorizma, prekograničnog kriminala i nezakonite migracije.

đena odlukom, čija će usklađenost sa Direktivom o zaštiti podataka za policiju i tela krivičnog pravosuđa morati da se procene. Tela nadležna za nadzor takvih prenosa podataka su domaća nadzorna tela za zaštitu podataka.

Okvirna odluka 2006/960/PUP – Švedska inicijativa

Okvirna odluka 2006/960/PUP (Švedska inicijativa)[789] predstavlja još jedan primer prekogranične saradnje u pogledu razmene podataka koje tela nadležna za održavanje javnog reda i mira poseduju na domaćem nivou. Švedska inicijativa posebno je usmerena na razmenu obaveštajnih podataka i informacija tako da se njenim članom 8. propisuju posebni propisi o zaštiti podataka.

U skladu sa tim instrumentom, upotreba razmenjenih informacija i obaveštajnih podataka mora podlegati domaćim odredbama za zaštitu podataka u državi članici koja prima informacije, u skladu sa istim propisima koji bi važili i da su podaci prikupljeni u toj državi članici. U članu 8. dalje se navodi da prilikom dostavljanja informacija i obaveštajnih podataka telo nadležno za održavanje javnog reda i mira može, u skladu sa svojim domaćiim zakonodavstvom, odrediti uslove za njihovu upotrebu telu nadležnom za održavanje javnog reda i mira koje ih prima. Ti uslovi se mogu primenjivati i na izveštavanje o rezultatima istrage o krivičnom delu ili operacijama prikupljanja obaveštajnih podataka o krivičnom delu za koje je bila potrebna razmena informacija i obaveštajnih podataka. Međutim, u slučajevima u kojima se domaćim zakonodavstvom propisuju izuzeća od ograničenje upotrebe (npr. za pravosudna tela, zakonodavna tela itd.), informacije i obaveštajni podaci mogu se upotrebljavati samo posle prethodnog savetovanja sa državom članicom koja ih dostavlja.

Dostavljene informacije i obaveštajni podaci mogu se upotrebljavati:

- za svrhe za koje su dostavljeni ili
- za sprečavanje neposredne i ozbiljne opasnosti za javnu bezbednost.

Obrada u druge svrhe može se dozvoliti samo uz prethodno odobrenje države članice koja ih dostavlja.

789 Savet Evropske unije (2006), Okvirna odluka Saveta 2006/960/PUP od 18. decembra 2006. o pojednostavljenju razmene informacija i obaveštajnih podataka između tela zaduženih za izvršavanje zakona u državama članicama Evropske unije, SL L 386/89 od 29. decembra 2006.

U Švedskoj inicijativi dalje se navodi da se obrađeni lični podaci moraju zaštititi u skladu sa međunarodnim instrumentima kao što su:

- Konvencija Saveta Evrope o zaštiti pojedinaca pri automatskoj obradi ličnih podataka[790],
- Dodatni protokol uz tu Konvenciju od 8. novembra 2001. koji se tiče nadzornih tela i prekograničnih prenosa podataka[791],
- Preporuka br. R(87) 15 Saveta Evrope o korišćenju ličnih podataka u sektoru policije[792].

Direktiva Evropske unije o evidenciji podataka o putnicima

Podaci iz evidencije podataka o putnicima (EPP) odnose se na informacije o putnicima u vazdušnom saobraćaju koji se prikupljaju i čuvaju u sistemima rezervacija i kontrole odlazaka avio-prevoznika u njihove sopstvene komercijalne svrhe. Oni sadrže nekoliko različitih vrsta podataka, kao što su datumi putovanja, plan putovanja, informacije o kartama, podaci za kontakt, informacije o putničkoj agenciji putem koje je let rezervisan, informacije o načinu plaćanja, broj sedišta i informacije o prtljagu[793]. Obrada podataka iz evidencije podataka o putnicima može pomoći telima nadležnim za održavanje javnog reda i mira da identifikuju poznate ili potencijalne osumnjičene i izvrše procene na osnovu obrazaca putovanja i drugih pokazatelja koji se obično povezuju sa kriminalnim aktivnostima. Analiza podataka iz evidencije takođe omogućava retrospektivno praćenje pravaca putovanja i kontakata osoba koje su osumnjičene za učestvovanje u kriminalnim aktivnostima, što telima nadležnim za održavanje javnog reda i mira može pomoći u otkrivanju kriminalnih mreža[794]. EU je zaključila određene sporazume sa trećim zemljama u svrhu razmene podataka iz evidencije podataka o putnicima, kako je objašnjeno u delu 7.

790 Savet Evrope (1981), Konvencija o zaštiti pojedinaca pri automatskoj obradi ličnih podataka, ETS br. 108.

791 Savet Evrope (2001), Dodatni protokol uz Konvenciju o zaštiti pojedinaca pri automatskoj obradi ličnih podataka, koji se tiče nadzornih tela i prekograničnih prenosa podataka, ETS br. 108.

792 Savet Evrope (1987), Preporuka br. R(87) 15 Odbora ministara o korišćenju ličnih podataka u sektoru policije (koju je doneo Odbor ministara 17. septembra 1987. na 410. sastanku zamenika ministara).

793 Evropska komisija (2011), Predlog direktive Evropskog parlamenta i Saveta o upotrebi podataka iz evidencije podataka o putnicima (PNR) u svrhu sprečavanja, otkrivanja, istrage i krivičnog gonjenja krivičnih dela terorizma i teških krivičnih dela, COM(2011) 32 final, Bruxelles, 2. februara 2011, str. 1.

794 Evropska komisija (2015), *Fact Sheet Fighting terrorism at EU level, an overview of Commission's actions, measures and initiatives* (Informativni list „Borba protiv terorizma na nivou EU: pregled delovanja, mera i inicijativa Komisije"), Bruxelles, 11. januara 2015.

Osim toga, Unija je uvela i obradu podataka iz EPP-a na području EU u sklopu Direktive 2016/681/EU o upotrebi podataka iz evidencije podataka o putnicima (EPP) u svrhu sprečavanja, otkrivanja, istrage i krivičnog gonjenja krivičnih dela terorizma i teških krivičnih dela (Direktiva EU o evidenciji podataka o putnicima)[795]. Tom Direktivom se avio-prevoznicima propisuju obaveze prenosa podataka iz EPP-a nadležnim telima i uspostavljaju stroge mere za zaštitu podataka za potrebe obrade i prikupljanja takvih podataka. Direktiva EU o evidenciji podataka o putnicima primenjuje se na međunarodne letove u EU i iz EU, kao i na letove unutar Unije ako država članica tako odluči[796].

Prikupljeni podaci iz EPP-a smeju da sadrže samo informacije dozvoljene Direktivom EU o evidenciji podataka o putnicima. Moraju se čuvati u posebnoj jedinici za informacije na sigurnoj lokaciji u svakoj državi članici. Podaci iz EPP-a moraju se depersonalizovati šest meseci pošto ih avio-prevoznik prenese i čuvati najviše pet godina[797]. Podaci iz EPP-a razmenjuju se među državama članicama, između država članica i Europol-a kao i s trećim zemljama, ali samo na osnovu pojedinih slučajeva.

Prenos i obrada podataka iz EPP-a i prava zaštićena za ispitanike moraju biti u skladu sa Direktivom o zaštiti podataka za policiju i tela krivičnog pravosuđa, pa se njima mora obezbediti visok nivo zaštite privatnosti ličnih podataka koji se propisuje Poveljom, Modernizovanom Konvencijom br. 108 i EKLJP-om.

Nezavisna domaća nadzorna tela, koja su nadležna na osnovu Direktive o zaštiti podataka za policiju i tela krivičnog pravosuđa, takođe su odgovorna za savetovanje o odredbama koje donesu države članice i praćenje njihove primene, shodno Direktivi EU o evidenciji podataka o putnicima.

Zadržavanje telekomunikacionih podataka

Prema Direktivi o zadržavanju podataka[798], koja je proglašena nevažećom 8. aprila 2014. u okviru predmeta *Digital Rights Ireland*, pružaoci komunikacionih usluga bili su dužni da stave na raspolaganje metapodatke u posebnu svrhu

795 Direktiva (EU) 2016/681 Evropskog parlamenta i Saveta od 27. aprila 2016. o upotrebi podataka iz evidencije podataka o putnicima (PNR) u svrhu sprečavanja, otkrivanja, istrage i krivičnog gonjenja krivičnih dela terorizma i teških krivičnih dela, SL 2016 L 119, str. 132.

796 Direktiva o evidenciji podataka o putnicima, L 119, str. 132, član 1. stav 1 i član 2. stav 1.

797 *Ibid.*, član 12. stav 1 i član 12. stav 2.

798 Direktiva 2006/24/EZ Evropskog parlamenta i Saveta od 15. marta 2006. o zadržavanju podataka dobijenih ili obrađenih u vezi s pružanjem javno dostupnih elektronskih komunikacionih usluga ili javnih komunikacionih mreža i o izmeni Direktive 2002/58/EZ, SL 2006 L 105.

suzbijanja teškog kriminala, tokom perioda od najmanje šest meseci i najviše 24 meseca, bez obzira na to da li su pružaocu ti podaci i dalje bili potrebni u svrhu naplate ili tehničkog pružanja usluge.

Zadržavanje telekomunikacionih podataka predstavlja jasno mešanje u pravo na zaštitu podataka[799]. Da li je takvo mešanje opravdano osporavalo se u nekoliko sudskih postupaka u državama članicama EU[800].

Primer: U predmetu *Digital Rights Ireland* i *Kärntner Landesregierung i drugi*[801], grupa Digital Rights i g. Zajtlinger pokrenuli su sudski postupak pred Visokim sudom u Irskoj, odnosno pred Ustavnim sudom u Austriji, osporavajući zakonitost domaćih mera kojima se omogućava zadržavanje elektronskih telekomunikacionih podataka. Grupa Digital Rights zatražila je od irskog suda da proglasi nevažećom Direktivu 2006/24 i deo domaćeg krivičnog prava u vezi sa terorističkim krivičnim delima. Na sličan su način g. Zajtlinger i više od 11 000 drugih tužilaca osporili i zatražili poništavanje odredbe austrijskog zakonodavstva o telekomunikacijama kojim je prenesena Direktiva 2006/24.

Rešavajući po gornjim prethodnim pitanjima, SPEU je proglasio Direktivu o zadržavanju podataka nevažećom. Prema SPEU, podaci koji su se mogli zadržavati na osnovu Direktive pružali su tačne informacije o pojedincima kada su se razmatrali kao celina. SPEU je zatim razmatrao ozbiljnost mešanja u osnovna prava na poštovanje privatnog života i zaštitu ličnih podataka. Zaključio je da se zadržavanjem podataka ostvaruje cilj javnog interesa, odnosno borbe protiv teškog kriminala, a time i javne bezbednosti. Uprkos tome, SPEU je utvrdio da je zakonodavac EU donošenjem Direktive povredio načelo srazmernosti. Iako je Direktiva mogla da bude primereno sredstvo za ostvarenje željenog cilja, „opsežno i posebno ozbiljno mešanje Direktive u osnovna prava na poštovanje privatnosti i zaštitu ličnih podataka nije dovoljno ograničeno kako bi se obezbedilo da je mešanje zaista ograničeno na ono što je strogo nužno".

799 EDPS (2011.), Mišljenje od 31. maja 2011. o Evaluacionom izveštaju Komisije Savetu i Evropskom parlamentu o Direktivi o zadržavanju podataka (Direktiva 2006/24/EZ), 31. maja 2011.

800 Nemačka, Savezni ustavni sud (Bundesverfassungsgericht), *1 BvR 256/08*, 2. marta 2010.; Rumunija, Savezni ustavni sud (Curtea Constituțională a României), br. 1258, 8. oktobra 2009.; Češka Republika, Ustavni sud (Ústavní soud České republiky), *94/2011 Coll.*, 22. marta 2011.

801 SPEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr. i Kärntner Landesregierung i dr.* [VV], 8. aprila 2014., stav 65.

Zadržavanje podataka dozvoljeno je, u nedostatku posebnog zakonodavstva o zadržavanju podataka, kao izuzeće od poverljivosti telekomunikacionih podataka na osnovu Direktive 2002/58/EZ (Direktiva o privatnosti i elektronskim komunikacijama)[802], kao preventivna mera, ali mora se vršiti isključivo u svrhu borbe protiv teških krivičnih dela. Takvo zadržavanje podataka mora biti ograničeno na ono što je strogo nužno s obzirom na kategorije zadržanih podataka, obuhvaćeno sredstvo komunikacije, dotične osobe i odabrani period zadržavanja. Domaća tela mogu imati pristup zadržanim podacima u strogo kontrolisanim uslovima, uključujući prethodni pregled nezavisnog tela. Podaci se moraju čuvati unutar EU.

Primer: Posle presude u predmetu *Digital Rights Ireland* i *Kärntner Landesregierung i drugi*[803] pred SPEU su se našla dodatna dva predmeta u vezi s opštom obavezom koja je u Švedskoj i Ujedinjenom Kraljevstvu nametnuta pružaocima elektronskih komunikacionih usluga za zadržavanje telekomunikacionih podataka, kako je bilo propisano Direktivom o zadržavanju podataka koja je proglašena nevažećom. U predmetima *Tele2 Sverige* i *Home Department protiv Toma Watsona i drugih*[804] SPEU je utvrdio da domaće zakonodavstvo kojim se propisuje opšte i neselektivno zadržavanje podataka bez uslovljavanja bilo kakvog odnosa između podataka koji se moraju zadržati i pretnje javnoj bezbednosti, kao i bez utvrđivanja bilo kakvih uslova – npr. perioda zadržavanja, geografskog područja, grupe lica za koje je verovatno da će biti uključene u teška krivična dela – premašuje granice strogo nužnog i ne može se smatrati opravdanim u demokratskom društvu, kako se propisuje Direktivom 2002/58/EZ, kada se tumači u smislu Povelje EU o osnovnim pravima.

Mogućnosti

U januaru 2017. Evropska komisija objavila je Predlog uredbe o poštovanju privatnog života i zaštiti ličnih podataka u elektronskim komunikacijama, kojom bi se stavila

802 Direktiva 2002/58/EZ Evropskog parlamenta i Saveta od 12. jula 2002. o obradi ličnih podataka i zaštiti privatnosti u oblasti elektronskih komunikacija (Direktiva o privatnosti i elektronskim komunikacijama), SL 2002 L 201.

803 SPEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr. i Kärntner Landesregierung i dr.* [VV], 8. aprila 2014.

804 SPEU, spojeni predmeti C-203/15 i C-698/15, *Tele2 Sverige AB protiv Post- och telestyrelsen i Secretary of State for the Home Department protiv Toma Watsona i drugih* [VV], 21. decembra 2016.

van snage i zamenila Direktiva 2002/58/EZ[805]. Predlog ne sadrži nikakve posebne odredbe o zadržavanju podataka. Međutim, u njemu se utvrđuje da države članice mogu zakonom ograničiti određene obaveze i prava na osnovu Uredbe ako takvo ograničenje čini nužnu i srazmernu meru za zaštitu posebnih javnih interesa, uključujući nacionalnu sigurnost, odbranu, javnu bezbednost i sprečavanje, istragu, otkrivanje i gonjenje krivičnih dela ili izvršavanja krivičnopravnih sankcija[806]. Tako bi države članice mogle da zadrže ili stvore domaće okvire za zadržavanje podataka kojima se utvrđuju ciljane mere zadržavanja, u meri u kojoj bi takvi okviri bili u skladu sa pravom Unije, uzimajući u obzir sudsku praksu SPEU u vezi sa tumačenjem Direktive o privatnosti i elektronskim komunikacijama i Povelju EU o osnovnim pravima[807]. U vreme izrade ovog priručnika rasprave o donošenju Uredbe još su bile u toku.

Krovni sporazum između SAD i EU o zaštiti ličnih informacija razmenjenih u svrhe održavanja javnog reda i mira

Krovni sporazum između SAD i Evropske unije o obradi ličnih podataka u svrhu sprečavanja, istrage, otkrivanja i gonjenja krivičnih dela stupio je na snagu 1. februara 2017.[808] Krovnim sporazumom između SAD i EU nastoji se da se obezbedi visok nivo zaštite podataka za građane EU i istovremeno poboljša saradnja domaćih tela nadležnih za održavanje javnog reda i mira EU i SAD. Njime se dopunjuju postojeći sporazumi između EU i SAD i država članica i SAD zaključenih između tela zaduženih za održavanje javnog reda i mira tako da se istovremeno uspostavljaju jasni i usklađeni propisi za zaštitu podataka za buduće sporazume u toj oblasti. Kad je reč o tome, sporazumom se nastoji da se utvrdi trajan pravni okvir za olakšanu razmenu informacija.

Sam sporazum ne daje prikladnu pravnu osnovu za razmenu ličnih podataka, ali pruža odgovarajuće mere za zaštitu podataka pojedincima na koje se to odnosi.

---

805 Evropska komisija (2017.), Predlog uredbe Evropskog parlamenta i Saveta o poštovanju privatnog života i zaštiti ličnih podataka u elektronskim komunikacijama i stavljanju van snage Direktive 2002/58/EZ (Uredba o privatnosti i elektronskim komunikacijama), COM(2017) 10 final, Bruxelles, 10. januara 2017.

806 *Ibid.*, uvodna izjava 26.

807 Videti Memorandum s objašnjenjima o Predlogu uredbe o privatnosti i elektronskim komunikacijama COM(2017) 10 final, tačka 1.3.

808 Videti Savet EU (2016.) *‚Enhanced data protection rights for EU citizens in law enforcement cooperation: EU and US sign ‘Umbrella agreement’* (Poboljšana prava zaštite podataka za građane EU temeljem saradnje tela za izvršavanje zakonodavstva: potpisivanje „Krovnog sporazuma" između EU i SAD), saopštenje za medije 305/16, 2. juna 2016.

On obuhvata svu obradu ličnih podataka nužnu za sprečavanje, istragu, otkrivanje i gonjenje krivičnih dela, uključujući terorizam[809].

Sporazumom se utvrđuje više zaštitnih mera kako bi se obezbedilo da se lični podaci upotrebljavaju isključivo u svrhe utvrđene u Sporazumu. Njime se građanima EU posebno pruža sledeća zaštita:

- ograničenja upotrebe podataka: lični podaci mogu se upotrebljavati samo u svrhu sprečavanja, istrage, otkrivanja ili gonjenja krivičnih dela,
- zaštita od proizvoljne i neopravdane diskriminacije,
- dalji prenosi: za svaki dalji prenos u zemlju izvan SAD i EU ili međunarodnu organizaciju mora se dobiti prethodni pristanak nadležnog tela zemlje koja je izvorno prenela podatke,
- kvalitet podataka: lični podaci moraju da se čuvaju tako da se u obzir uzmu njihova tačnost, relevantnost, ažurnost i celovitost,
- bezbednost obrade, uključujući obaveštenje o povredama ličnih podataka,
- obrada osetljivih podataka dozvoljena je samo uz odgovarajuće zaštitne mere u skladu sa zakonom,
- periodi zadržavanja: lični podaci ne smeju se zadržavati duže nego što je nužno ili primereno,
- prava na pristup i ispravku: svaki pojedinac ima pravo na pristup svojim ličnim podacima pod određenim uslovima tako da će moći da zatraži ispravljanje podataka ako su netačni,
- za automatizovane odluke potrebne su odgovarajuće zaštitne mere, uključujući mogućnost ljudske intervencije,
- delotvoran nadzor, uključujući saradnju između nadzornih tela EU i SAD kao i

809 Sporazum između Sjedinjenih Američkih Država i Evropske unije o zaštiti ličnih informacija u vezi sa sprečavanjem, istragom, otkrivanjem i gonjenjem krivičnih dela od 18. maja 2016, (OR.en) 8557/16, član 3. stav 1. Videti i Obaveštenje Komisije o pregovorima o sporazumu za zaštitu podataka između EU i SAD od 26. maja 2010., MEMO/10/216 i Saopštenje za medije Evropske komisije (2010.) o visokim standardima privatnosti u sporazumu o zaštiti podataka između EU i SAD od 26. maja 2010., IP/10/609.

- sudska zaštita i provedivost: građani EU imaju pravo[810] da zatraže sudsku zaštitu pred sudovima u SAD u slučajevima u kojima nadležna tela SAD uskrate pristup ili ispravku ili nezakonito otkriju njihove lične podatke.

Prema „Krovnom sporazumu" uspostavljen je i sistem za obaveštavanje nadležnog nadzornog tela države članice EU u kojoj se nalaze dotični pojedinci o svim povredama zaštite podataka, kada je to potrebno. Pravnim zaštitnim merama koje su utvrđene Sporazumom obezbeđuje se jednako postupanje prema građanima EU u SAD u slučaju povrede privatnosti[811].

8.3.1. Zaštita podataka u pravosudnim telima i agencijama EU nadležnim za održavanje javnog reda i mira

Europol

Europol, telo za održavanje javnog reda i mira Evropske unije sa sedištem u Hagu, ima Europolove nacionalne jedinice (ENJ) u svakoj državi članici. Europol je osnovan 1998. godine. Njegov trenutni pravni status institucije Evropske unije zasniva se na Uredbi o Agenciji Evropske unije za saradnju tela nadležnih za održavanje javnog reda i mira (Uredba o Europolu)[812]. Cilj Europola je da pomogne u sprečavanju i istrazi organizovanog kriminala, terorizma i drugih oblika teških krivičnih dela koja utiču na dve ili više država članica, a koja su navedena u Prilogu I Uredbe o Europolu. To se postiže razmenom informacija i njegovom ulogom informacione centrale EU koja daje analize obaveštajnih podataka i procene pretnji.

Radi ostvarenja svojih ciljeva Europol je uspostavio Europolov informacioni sistem sa bazom podataka na osnovu koje države članice razmenjuju kriminalističke obaveštajne

810 Zakon SAD o sudskoj zaštiti (US Judicial Redress Act) stupio je na snagu potpisom predsednika Obame 24. februara 2016.

811 Evropski nadzornik za zaštitu podataka izdao je Mišljenje o Sporazumu između EU i SAD kojim je, između ostalog, preporučio sledeće izmene: 1) dodavanje teksta „u posebne svrhe u koje su preneseni" u član koji se odnosi na zadržavanje podataka ne duže nego što je nužno i primereno 2) izuzimanje grupnog prenosa osetljivih podataka, što je možda moguće. Videti Evropski nadzornik za zaštitu podataka, Mišljenje 1/2016 (dostupno na engleskom jeziku), *Preliminarno mišljenje o Sporazumu između Sjedinjenih Američkih Država i Evropske unije o zaštiti ličnih informacija u vezi sa sprečavanjem, istragom, otkrivanjem i gonjenjem krivičnih dela*, član 35.

812 Uredba (EU) 2016/794 Evropskog parlamenta i Saveta od 11. maja 2016. o Agenciji Evropske unije za saradnju tela za izvršavanje zakonodavstva (Europol) i zameni i stavljanju van snage odluka Saveta 2009/371/PUP, 2009/934/PUP, 2009/935/PUP, 2009/936/PUP i 2009/968/PUP, SL 2016 L 135, str. 53.

podatke i informacije putem svojih ENU. Europolov informacioni sistem može se upotrebljavati radi stavljanja na raspolaganje podataka koji se odnose na: osobe koje su osumnjičene ili osuđene za krivično delo u nadležnosti Europola ili osobe za koje se opravdano sumnja da će takva dela počiniti. Europol i ENU mogu direktno da unose podatke u Europolov sistem informacija i preuzimaju ih iz njega. Podatke može izmeniti, ispraviti ili izbrisati samo strana koja ih je unela u sistem. Tela EU, treće zemlje i međunarodne organizacije takođe mogu davati informacije Europolu.

Europol može prikupljati informacije i lične podatke i iz javno dostupnih izvora kao što je internet. Prenosi ličnih podataka telima EU dozvoljeni su samo ako je to nužno za izvršavanje zadatka Europola ili tela EU koje podatke prima. Prenosi ličnih podataka u treće zemlje ili međunarodne organizacije dozvoljeni su samo ako Evropska komisija odluči da ta zemlja ili međunarodna organizacija obezbeđuje odgovarajuću nivo zaštite podataka („odluka o primerenosti") ili ako postoji međunarodni sporazum ili sporazum o saradnji. Europol može da dobija i obrađuje lične podatke privatnih strana i fizičkih lica pod strogo određenim uslovima prema kojima te podatke mora prenositi ENU u skladu sa svojim domaćim zakonodavstvom, kontakt tačka u trećoj zemlji ili međunarodna organizacija sa kojom je uspostavljena saradnja putem sporazuma o saradnji, ili telo treće zemlje ili međunarodna organizacija koja podleže odluci o primerenosti ili sa kojom je EU sklopila međunarodni sporazum. Sve razmene informacija vrše se putem mrežne aplikacije za bezbednu razmenu informacija (*Secure Information Exchange Network Application*, SIENA).

Kao odgovor na nove pojave, unutar Europola osnovani su specijalizovani centri. Evropski centar za kibernetički kriminal osnovan je unutar Europola 2013. godine.[813] Centar ima ulogu središta Evropske unije za kibernetički kriminal, čime se omogućava brže reagovanje u slučaju internet zločina, razvijanje i primena digitalnih forenzičkih rešenja i vrši najbolja praksa u istragama kibernetičkog kriminala. Centar se bavi kibernetičkim kriminalom koji:

- učine organizovane grupe radi ostvarivanja velike kriminalne dobiti, kao što je internet prevara,
- prouzrokuje veliku štetu žrtvi, poput seksualnog iskorišćavanja dece putem interneta,
- utiče na ključnu infrastrukturu ili informacione sisteme u Evropskoj uniji.

813 Videti i EDPS (2012), Mišljenje Nadzornika za zaštitu podataka o saopštenju Evropske komisije Savetu i Evropskom parlamentu o osnivanju Evropskog centra za sajber kriminal, Bruxelles, 29. juna 2012.

Evropski centar za borbu protiv terorizma (ECBT) osnovan je u januaru 2016. radi pružanja operativne pomoći državama članicama u istragama povezanim s terorističkim krivičnim delima. Centar vrši unakrsne provere aktuelnih operativnih podataka u odnosu na podatke koje Europol već poseduje, čime se brzo otkrivaju tragovi finansiranja, i analizira sve dostupne pojedinosti istrage kako bi pomogao u stvaranju strukturiranog pregleda terorističke mreže[814].

Evropski centar za borbu protiv krijumčarenja migranata (ECBKM) osnovan je u februaru 2016. godine, posle sastanka Saveta u novembru 2015., kako bi se državama članicama pomoglo u otkrivanju i uništavanju zločinačkih mreža uključenih u krijumčarenje migranata. Centar deluje kao informaciona centrala koja pruža pomoć kancelarijama Regionalne jedinice EU u Kataniji (Italija) i Pireju (Grčka), koji pomažu domaćim telima u nekoliko oblasti, uključujući deljenje obaveštajnih podataka, istrage krivičnih dela i gonjenja zločinačkih mreža za krijumčarenje ljudi[815].

Sistem zaštite podataka kojim se uređuju aktivnosti Europola proširen je i zasniva se na načelima Uredbe o zaštiti podataka u institucijama EU[816], a u skladu je i sa Direktivom o zaštiti podataka za policiju i tela krivičnog pravosuđa, modernizovanom Konvencijom br. 108 i Preporukom o policiji.

Obrada ličnih podataka u pogledu žrtava krivičnih dela, svedoka ili drugih lica koja mogu dati informacije o krivičnim delima ili u pogledu lica mlađih od 18 godina dozvoljeno je ako je to izričito nužno i srazmerno radi sprečavanja ili suzbijanja kriminaliteta koji potpada pod ciljeve Europola[817]. Obrada osetljivih ličnih podataka zabranjena je osim ako je to izričito nužno i srazmerno radi sprečavanja ili suzbijanja vrsta krivičnih dela obuhvaćenih ciljevima Europola i ako ti podaci dopunjavaju druge lične podatke koje je Europol obradio[818]. U oba slučaja samo Europol može pristupiti relevantnim podacima[819].

814 Videti Europolovu internet stranicu za ECTC.

815 Videti Europolovu internet stranicu za EMSC.

816 Uredba (EZ) br. 45/2001 Evropskog parlamenta i Saveta od 18. decembra 2000. o zaštiti pojedinaca u vezi s obradom ličnih podataka u institucijama i telima Zajednice i o slobodnom kretanju takvih podataka, SL 2001 L 8.

817 Uredba o Europolu, član 30. stav 1.

818 *Ibid*., član 30. stav 2.

819 *Ibid*., član 30. stav 3.

Čuvanje podataka dozvoljeno je samo onoliko dugo koliko je potrebno i srazmerno, a dalje čuvanje se preispituje svake tri godine. Bez tog preispitivanja podaci se automatski brišu[820].

Europol u određenim uslovima može direktno da prenosi lične podatke telu EU ili telu treće zemlje ili međunarodnoj organizaciji[821]. Ako bi kršenje ličnih podataka verovatno znatno i negativno uticalo na prava i slobode dotičnih ispitanika, o tome se moraju obavestiti bez nepotrebnog odlaganja[822]. Na nivou država članica imenovaće se domaće nadzorno telo koje će nadgledati Europolovu obradu ličnih podataka[823].

EDPS je odgovoran za nadzor i obezbeđivanje zaštite osnovnih prava i sloboda fizičkih lica u pogledu obrade ličnih podataka koju obavlja Europol, kao i za savetovanje Europola i ispitanika o svim pitanjima koja se odnose na obradu ličnih podataka. U tu svrhu EDPS deluje kao telo za istrage i tužbe i blisko sarađuje sa domaćim nadzornim telima[824]. EDPS i domaća nadzorna tela sastaju se najmanje dvaput godišnje u okviru Odbora za saradnju koji ima savetodavnu funkciju[825]. Države članice dužne su da zakonom uspostave nadzorno telo koje je nadležno za praćenje dopustivosti prenosa ličnih podataka sa nivoa države Europolu, kao i prikupljanja ličnih podataka i saopštavanja Europolu ličnih podataka što čine države članice[826]. Države članice takođe moraju obezbediti da domaće nadzorno telo može da deluje sasvim nezavisno u ispunjavanju svojih zadataka i dužnosti na osnovu Uredbe o Europolu[827]. Kako bi proverio zakonitost obrade podataka, samostalno pratio svoje aktivnosti i obezbedio celovitost i sigurnost podataka, Europol vodi evidenciju ili dokumentaciju o svojim aktivnostima obrade podataka. Ta evidencija sadrži informacije o postupcima obrade u sistemima automatizovane obrade, a odnosi se na sakupljanje, izmene, pristup, otkrivanje, kombinaciju i brisanje[828].

820 *Ibid.,* član 31.

821 *Ibid.*, član 24. odnosno član 25.

822 *Ibid.*, član 35.

823 Uredba o Europolu, član 42.

824 *Ibid.*, član 43. i član 44.

825 *Ibid.*, član 45.

826 *Ibid.*, član 42. stav 1.

827 *Ibid.*, član 42. stav 1.

828 *Ibid.*, član 40.

Žalba na odluku EDPS-a može se podneti SPEU[829]. Svako lice koje je pretrpelo štetu kao posledicu nezakonitih radnji obrade podataka ima pravo na dobijanje nadoknade za pretrpljenu štetu, bilo od Europola ili od odgovorne države članice EU, tako da pokrene postupak pred SPEU (prvi slučaj) ili pred nadležnim domaćim sudom (drugi slučaj)[830]. Usto, specijalizovana Zajednička grupa za parlamentarni nadzor (ZGPN) domaćih parlamenata i Evropskog parlamenta može da nadgleda aktivnosti Europola[831]. Svaki pojedinac ima pravo na pristup svim ličnim podacima koje Europol čuva o njemu, kao i pravo da zatraži da se ti lični podaci provere, isprave ili obrišu. Ta prava mogu podlegati izuzećima i ograničenjima.

Eurodžast (Eurojust)

Eurodžast je telo Evropske unije osnovano 2002. godine, sa sedištem u Hagu. Ono unapređuje pravosudnu saradnju u istragama i gonjenjima teških krivičnih dela koja uključuju barem dve države članice[832]. Eurodžast je nadležan za sledeće:

- podsticanje i unapređivanje koordinacije istraga i gonjenja među nadležnim telima različitih država članica,

- olakšavanje izvršavanja zahteva i odluka koji se odnose na pravosudnu saradnju.

Funkcije Eurodžsta vrše nacionalni članovi. Svaka država članica imenuje po jednog sudiju ili tužioca Eurodžasta sa potrebnim stručnim veštinama za izvršavanje zadataka potrebnih za podsticanje i unapređenje pravosudne saradnje. Status tog sudije ili tužioca podleže domaćem zakonodavstvu. Osim toga, nacionalni članovi zajednički su okupljeni u kolegijum radi izvršavanja posebnih Eurodžastovih zadataka.

Eurodžast može obrađivati lične podatke ako je to potrebno da bi ostvario svoje ciljeve. Međutim, ta mogućnost je ograničena na određene informacije u vezi sa

829 *Ibid*., član 48.

830 *Ibid*., član 50.

831 *Ibid*., član 51.

832 Savet Evropske unije (2002.), Odluka Saveta 2002/187/PUP od 28. februara 2002. kojom se osniva Eurodžast s ciljem jačanja borbe protiv teških krivičnih dela, SL 2002 L 63; Savet Evropske unije (2003.), Odluka Saveta 2003/659/PUP od 18. juna 2003. o izmeni Odluke 2002/187/PUP kojom se osniva Eurodžast sa ciljem jačanja borbe protiv teških krivičnih dela, SL 2003 L 44; Savet Evropske unije (2009.), Odluka Saveta 2009/426/PUP od 16. decembra 2008. o jačanju Eurodžasta i izmeni Odluke 2002/187/PUP o osnivanju Eurodžasta sa ciljem jačanja borbe protiv teških krivičnih dela, SL 2009 L 138 (odluke o Eurojustu).

licima osumnjičenim za činjenje krivičnog dela ili učestvovanje u njemu ili licima osuđenim za krivično delo u nadležnosti Eurodžasta. Eurodžast može obrađivati i informacije u vezi sa svedocima ili žrtvama krivičnih dela iz nadležnosti Eurodžasta[833]. U izuzetnim okolnostima i tokom ograničenog vremenskog perioda Eurodžast može da obrađuje širi raspon ličnih podataka u vezi s okolnostima krivičnog dela ako se takvi podaci neposredno odnose na istragu koja je u toku. U okviru svoje oblasti nadležnosti Eurodžst može da sarađuje s drugim institucijama, telima i agencijama Evropske unije i sa njima razmenjuje lične podatke. Eurodžst može da sarađuje i razmenjuje podatke i ss trećim zemljama i organizacijama.

U vezi sa zaštitom podataka, Eurodžast mora da garantuje nivo zaštite barem jednak načelima iz modernizovane Konvencije br. 108 i njenim kasnijim izmenama. Pri razmeni podataka moraju se poštovati posebna pravila i ograničenja uvedena sporazumom o saradnji ili radnim dogovorom u skladu s Odlukama Saveta o Eurodžastu i Pravilima o zaštiti podataka u Eurodžastu[834].

U okviru Eurodžasta osnovano je Zajedničko nadzorno telo (ZNT) sa zadatkom nadzora obrade ličnih podataka koju vrši Eurodžast. Pojedinci mogu da se žale Zajedničkom nadzornom telu ako nisu zadovoljni Eurodžastovom odlukom u vezi sa zahtevom za pristup, ispravku, blokiranje ili brisanje ličnih podataka. Ako Eurdžaust takve lične podatke obrađuje nezakonito, snosi odgovornost u skladu sa domaćim zakonodavstvom države članice u mestu njegovog sedišta, Holandiji, za štetu prouzrokovanu ispitaniku.

Mogućnosti

Evropska komisija iznela je predlog uredbe o reformi Eurodžasta u julu 2013. godine. Predlog je bio dopunjen predlogom o uspostavljanju Kancelarije evropskog javnog tužioca (videti dalje u tekstu). Tom uredbom se nastoji da se pojednostave funkcije i struktura kako bi bile u skladu sa Lisabonskim ugovorom. Zatim, cilj reforme je da se uspostavi jasna podela između operativnih zadataka Eurodžasta, koje obavlja njegov Kolegijum, i njegovih administrativnih zadataka. Time će se i državama članicama omogućiti da se više posvete operativnim zadacima. Osnovaće se novi Izvršni odbor koji će pomagati Kolegijumu u obavljanju administrativnih zadataka[835].

833 Pročišćena verzija Odluke Saveta 2002/187/PUP kako je izmenjena Odlukom Saveta 2003/659/PUP i Odlukom Saveta 2009/426/PUP, član 15. stav 2.

834 Poslovnik o obradi i zaštiti ličnih podataka u Eurodžastu, SL 2005 C 68/01, 19. marta 2005., str. 1.

835 Videti internet stranicu Komisije posvećenu Eurodžastu.

Kancelarija evropskog javnog tužioca

Države članice imaju isključivu nadležnost nad gonjenjem krivičnih dela prevare i nedozvoljenog korišćenja budžeta EU, koja mogu imati i prekogranične posledice. Raste važnost istrage, krivičnog gonjenja i podizanja optužnica protiv učinilaca takvih krivičnih dela, naročito s obzirom na trenutnu ekonomsku krizu[836]. Evropska komisija donela je predlog Uredbe o osnivanju nezavisne Kancelarije evropskog javnog tužioca (KEJT)[837] sa ciljem borbe protiv krivičnih dela koja utiču na finansijske interese EU. KEJT će se osnovati u sklopu postupka pojačane saradnje, koji omogućava da najmanje devet država članica uspostavi napredni nivo saradnje u okviru struktura EU bez uključivanja ostalih zemalja EU[838]. Belgija, Bugarska, Kipar, Češka, Estonija, Finska, Francuska, Grčka, Hrvatska, Letonija, Litvanija, Luksemburg, Nemačka, Portugalija, Rumunija, Slovačka, Slovenija i Španija pridružile su se pojačanoj saradnji, a Austrija i Italija izrazile su nameru da se pridruže[839].

KEJT će biti nadležan za istragu i gonjenje krivičnih dela prevare i drugih krivičnih dela u EU koja utiču na finansijske interese EU, sa ciljem delotvorne koordinacije istraga i gonjenja nezavisno od domaćih pravnih poredaka i sa ciljem poboljšanja iskorišćavanja resursa i razmene informacija na evropskom nivou[840].

KEJT će predvoditi evropski javni tužilac i najmanje po jedan imenovani evropski tužilac u svakoj državi članici zadužen za sprovođenje istraga i gonjenja u toj državi članici.

U Predlogu se utvrđuju snažne zaštitne mere kojima se garantuju prava lica uključenih u istrage KEJT-a kako su propisana domaćim zakonodavstvom, pravom EU i Poveljom EU o osnovnim pravima. Za istražne mere koje se uglavnom odnose na

836 Videti Evropska komisija (2013), Predlog uredbe Saveta o osnivanju Kancelarije evropskog javnog tužioca, COM(2013) 534 final, Bruxelles, 17. jula 2013, str. 1. i internet stranicu Komisije posvećenu EJT-u.

837 Evropska komisija (2013.), Predlog uredbe Veća o osnivanju Kancelarije evropskog javnog tužioca, COM(2013) 534 final, Bruxelles, 17. jula 2013.

838 Ugovor o funkcionisanju Evropske unije, član 86. stav 1. i član 329. stav 1.

839 Videti Savet Evropske unije (2017.), *„Postignut dogovor 20 država članica o pojedinostima uspostave Kancelarije evropskog javnog tužioca"*, saopšte- nje za medije, 8. juna 2017.

840 Evropska komisija (2013), Predlog uredbe Saveta o osnivanju Kancelarije evropskog javnog tužioca, COM(2013) 534 final, Bruxelles, 17. jula 2013, str. 1. i str. 50–51. Videti i internet stranicu Komisije posvećenu EJT-u.

osnovna prava biće potrebno prethodno odobrenje domaćeg suda[841]. Istrage KEJT-a podlegaće sudskom preispitivanju domaćih sudova[842].

Na obradu administrativnih ličnih podataka koju vrši KEJT primenjivaće se Uredba o zaštiti podataka u institucijama Evropske unije[843]. Za obradu ličnih podataka u vezi s operativnim pitanjima, kao što je Europol, KEJT će imati zaseban sistem zaštite podataka sličan onome kojim se uređuju aktivnosti Europola i Eurodžasta, budući da će izvršavanje funkcija KEJT-a uključivati obradu ličnih podataka s organima nadležnim za održavanje javnog reda i mira i tužilaštvom na nivou država članica. Pravila KEJT-a za zaštitu podataka zato su gotovo jednaka odredbama Direktive o zaštiti podataka za policiju i tela krivičnog pravosuđa. Prema Predlogu o osnivanju KEJT-a, obrada ličnih podataka mora biti u skladu sa načelima zakonitosti i pravičnosti, ograničenja svrhe, smanjenja količine podataka, tačnosti, celovitosti i poverljivosti. KEJT mora, koliko je to moguće, jasno razlikovati lične podatke različitih vrsta ispitanika, kao što su lica osuđena za krivična dela, lica koja su samo osumnjičena, žrtve i svedoci. Takođe mora nastojati da proveri kvalitet obrađenih ličnih podataka i razlikuje, koliko je to moguće, lične podatke na osnovu činjenica iz ličnih podataka i na osnovu ličnih procena.

Predlog sadrži odredbe o pravima ispitanika, tačnije pravima na informacije, pristup sopstvenim ličnim podacima, kao i na ispravku, brisanje i ograničenje obrade, tako da se njime utvrđuje da se takva prava mogu ostvarivati i posredno, putem EDPS-a. Predlog takođe otelotvoruje načela bezbednosti obrade i odgovornosti, kojima se uslovljava da KEJT izvrši odgovarajuće tehničke i organizacione mere kako bi obezbedila nivo sigurnosti koji odgovara rizicima obrade, vodi evidenciju o svim aktivnostima obrade i vrši procene efekta zaštite podataka pre same obrade ako postoji verovatnoća da će neka vrsta obrade (na primer, obrada koja uključuje nove tehnologije) prouzrokovati visok rizik za prava pojedinaca. Konačno, Predlogom se predviđa da Kolegijum imenuje službenika za zaštitu podataka koji mora biti uključen u sva pitanja u vezi sa zaštitom ličnih podataka i koji mora obezbediti postupanje KEJT-a u skladu sa svim merodavnim zakonodavstvom o zaštiti podataka.

841 Evropska komisija (2013), Predlog uredbe Saveta o osnivanju Kancelarije evropskog javnog tužioca, COM(2013) 534 final, Bruxelles, 17. jula 2013, član 26. stav 4.

842 *Ibid.*, član 36.

843 Uredba (EZ) br. 45/2001 Evropskog parlamenta i Saveta od 18. decembra 2000. o zaštiti pojedinaca u vezi s obradom ličnih podataka u institucijama i telima Zajednice i o slobodnom kretanju takvih podataka, SL 2001 L 8.

8.3.2. Zaštita podataka u zajedničkim informacionim sistemima na nivou Evropske unije

Osim razmene podataka među državama članicama i osnivanja specijalizovanih tela Evropske unije za suzbijanje prekograničnog kriminala, kao što su Europol, Eurodžast i KEJT, na nivou Evropske unije uspostavljeno je nekoliko zajedničkih informacionih sistema koji omogućavaju i olakšavaju saradnju i razmenu podataka između nadležnih domaćih tela i tela EU u posebne svrhe u oblastima zaštite granica, imigracija i azila, kao i carine. Kako je Šengenska zona prvobitno uspostavljena međunarodnim sporazumom nezavisnim od prava EU, tako je i Šengenski informacioni sistem (ŠIS) izrastao iz multilateralnih sporazuma, pa je naknadno obuhvaćen pravom EU. Vizni informacioni sistem (VIS), Eurodak, Eurosur i carinski informacioni sistem (CIS) nastali su kao instrumenti uređeni pravom EU.

Nadzor nad tim sistemima zajednički vrše domaća nadzorna tela i EDPS. Kako bi se obezbedio visoki nivo zaštite, ta tela sarađuju u okviru Koordinacionih grupa za nadzor (KGN), što se odnosi na sledeće opsežne informacione sisteme: 1) Eurodak; 2) Vizni informacioni sistem; 3) Šengenski informacioni sistem; 4) Carinski informacioni sistem i 5) Informacioni sistem unutrašnjeg tržišta[844]. KGN-ovi obično se sastaju dvaput godišnje, pod nadležnošću izabranog predsednika, i donose smernice, raspravljaju o prekograničnim predmetima ili donose zajedničke okvire za inspekcije.

Evropska agencija za opsežne informacione sisteme (eu-LISA)[845], osnovana 2012. godine, odgovorna je za operativno upravljanje Šengenskim informacionim sistemom druge generacije (ŠIS II), Viznim informacionim sistemom (VIS) i Eurodakom. Osnovni zadatak agencije eu-LISA je da obezbedi delotovoran, siguran i neprekidan rad informacionih sistema. Odgovorna je i za donošenje potrebnih mera bezbednosti sistema i podataka.

844 Videti internet stranicu o koordiniranju nadzora Evropskog nadzornika za zaštitu podataka (dostupnu na engleskom jeziku).

845 Uredba (EU) br. 1077/2011 Evropskog parlamenta i Saveta od 25. oktobra 2011. o osnivanju Evropske agencije za operativno upravljanje opsežnim informacionim sistemima u oblasti slobode, sigurnosti i pravde, SL 2011 L 286.

Šengenski informacioni sistem

Godine 1985. nekoliko država članica nekadašnje Evropske zajednice sklopilo je Sporazum sa državama Ekonomske unije Beneluksa, Nemačkom i Francuskom o postepenom ukidanju kontrola na zajedničkim granicama (Šengenski sporazum) kako bi se stvorio prostor za slobodno kretanje lica, neometan graničnim kontrolama unutar šengenskog prostora[846]. Kao protivteža pretnji javnoj bezbednosti usled otvaranja granica, uspostavljene su pojačane granične kontrole na spoljašnjim granicama šengenskog prostora, kao i uska saradnja domaće policije i pravosudnih tela.

Budući da je Šengenskom sporazumu pristupilo još država, šengenski sistem je konačno integrisan u pravni okvir Evropske unije Ugovorom iz Amsterdama[847]. Ta odluka je sprovedena 1999. godine. Najnovija verzija Šengenskog informacionog sistema, takozvani ŠIS II, puštena je u rad 9. aprila 2013. Trenutno se njime služi većina država članica EU[848], kao i Island, Lihtenštajn, Norveška i Švajcarska[849]. Europol i Eurodžst takođe imaju pristup sistemu ŠIS II.

ŠIS II sastoji se od centralnog sistema (C-ŠIS), nacionalnog sistema (N-ŠIS) u svakoj državi članici i komunikacione infrastrukture između centralnog sistema i nacionalnih sistema. C-ŠIS sadrži određene podatke o licima i predmetima koje unose države članice. ŠIS-om se služe domaćaa tela za graničnu kontrolu kao i policijska, carinska, vizna i pravosudna tela širom Šengenske zone. Svaka od država članica upravlja nacionalnom kopijom sistema C-ŠIS, poznatom kao nacionalni Šengenski informacioni sistem (N-ŠIS) koji se neprestano ažurira, čime se ažurira i C-ŠIS. U ŠIS-u postoje različite vrste upozorenja:

- lice nema pravo da uđe u Šengensku zonu ili da ostane u njemu,
- lice ili predmet traže pravosudni organi ili organi za održavanje javnog reda i mira (npr. evropski nalozi za hapšenje, zahtevi za skrivene provere),

846 Sporazum između vlada država Ekonomske unije Beneluksa, Savezne Republike Nemačke i Francuske Republike o postupnom ukidanju kontrola na zajedničkim granicama, SL 2000 L 239.

847 Evropske zajednice (1997), Ugovor iz Amsterdama o izmeni Ugovora o Evropskoj uniji, ugovorâ o osnivanju Evropskih zajednica i određenih s njima povezanih akata, SL 1997 C 340.

848 Hrvatska, Kipar i Irska vrše pripremne aktivnosti za pristupanje sistemu ŠIS II, ali još mu nisu pridružene. Videti informacije o Šengenskom informacionom sistemu dostupne na internet stranici Glavne uprave Evropske komisije za migracije i unutrašnje poslove.

849 Uredba (EZ) br. 1987/2006 Evropskog parlamenta i Saveta od 20. decembra 2006. o uspostavi, delovanju i korišćenju druge generacije Šengenskog informacionog sistema, SL 2006 L 381 (SIS II) i Savet Evropske unije (2007.), Odluka Saveta 2007/533/PUP od 12. juna 2007. o osnivanju, radu i korišćenju druge generacije Šengenskog informacionog sistema (SIS II), SL 2007 L 205.

- lice je prijavljeno kao nestalo ili

- roba, kao što su novčanice, automobili, kamioni, vatreno oružje i identifikacioni dokumenati, prijavljena je kao ukradena ili izgubljena imovina.

U slučaju upozorenja treba pokrenuti prateće aktivnosti putem kancelarije SIRENE. ŠIS II ima nove funkcionalnosti kao što je mogućnost unosa: biometrijskih podataka, poput otisaka prstiju i fotografija; novih vrsta upozorenja, poput ukradenih plovila, vazduhoplova, kontejnera ili sredstava plaćanja; pojačanih upozorenja o licima i predmetima; kopija evropskih naloga za hapšenje (ENH-ova) o licima traženim radi hapšenja, predaje ili izručenja.

ŠIS II zasniva se na dva akta koji se međusobno dopunjuju: Odluci o sistemu ŠIS II[850] i Uredbi o sistemu ŠIS II[851]. Zakonodavac EU primenjivao je različite pravne osnove za donošenje Odluke i Uredbe. Odlukom se uređuje upotreba sistema ŠIS II u svrhe obuhvaćene saradnjom policije i pravosudnih tela u krivičnim stvarima (nekadašnji treći stub EU). Uredba se primenjuje na postupke upozorenja koji potpadaju pod politike viza, azila, imigracija i druge politike koje se odnose na slobodno kretanje lica (nekadašnji prvi stub). Postupci upozorenja za svaki stub trebalo je da budu uređeni zasebnim aktima, budući da su navedena dva pravna akta donesena pre Ugovora iz Lisabona i ukidanja strukture stubova.

Oba pravna akta sadrže odredbe o zaštiti podataka. Odlukom o sistemu ŠIS II zabranjuje se obrada osetljivih podataka[852]. Obrada ličnih podataka obuhvaćena je modernizovanom Konvencijom br. 108[853]. Usto, lica imaju pravo na pristup ličnim podacima koji se odnose na njih, a koji se unosu u ŠIS II[854].

Uredbom o sistemu ŠIS II regulišu se uslovi i postupci za unos i obradu upozorenja u vezi s uskraćivanjem ulaska ili boravka lica koja nisu građani EU. Njome se, takođe, propisuju pravila za razmenu dopunskih i dodatnih informacija u svrhu ulaska u državu članicu ili boravka u njoj[855]. Uredba sadrži i odredbe o zaštiti podataka.

850 Odluka Saveta 2007/533/PUP od 12. juna 2007. o osnivanju, radu i korišćenju druge generacije Šengenskog informacionog sistema (SIS II), SL L 205, 7. avgusta 2007.

851 Uredba (EZ) br. 1987/2006 Evropskog parlamenta i Saveta od 20. decembra 2006. o uspostavi, delovanju i korišćenju druge generacije Šengenskog informacionog sistema (SIS II), SL L 381, 28. decembra 2006.

852 Odluka o sistemu ŠIS II, član 56.; Uredba o sistemu ŠIS II, član 40.

853 Odluka o sistemu ŠIS II, član 57.

854 Odluka o sistemu ŠIS II, član 58.; Uredba o sistemu ŠIS II, član 41.

855 Uredba o sistemu ŠIS II, član 2.

Osetljive kategorije podataka, utvrđene članom 9. stav 1. Opšte uredbe o zaštiti podataka, ne smeju da se obrađuju[856]. Uredba o sistemu ŠIS II sadrži i određena prava za ispitanika, odnosno:

- pravo na pristup ličnim podacima koji se odnose na ispitanika[857],
- pravo na ispravku netačnih podataka[858],
- pravo na brisanje nezakonito sačuvanih podataka[859], i
- pravo na informacije u slučaju izdatog upozorenja protiv ispitanika. Informacije se moraju dati u pisanom obliku i mora im se priložiti kopija ili pozivanje na domaću odluku na osnovu koje je izdato upozorenje[860].

Pravo na informacije ne dodeljuje se ako 1) lični podaci nisu dobijeni od predmetnog ispitanika i davanje informacija nije moguće ili bi zahtevalo nesrazmeran napor, 2) ako ispitanik već raspolaže informacijama ili 3) ako se domaćim pravom omogućava ograničenje na osnovu, između ostalog, zaštite nacionalne bezbednosti ili sprečavanja krivičnih dela[861].

U skladu i sa Odlukom o sistemu ŠIS II i sa Uredbom o sistemu ŠIS II, prava na pristup pojedinaca u vezi sa sistemom ŠIS II mogu se ostvariti u bilo kojoj državi članici tako da će se uređivati u skladu sa domaćim zakonodavstvom te države članice[862].

Primer: U predmetu *Dalea protiv Francuske*[863] podnosiocu predstavke je odbijen zahtev za vizu radi posete Francuskoj jer su francuske vlasti prijavile Šengenskom informacionom sistemu da mu se mora uskratiti ulazak u zemlju.

856 *Ibid.*, član 40.
857 *Ibid.*, član 41. stav 1.
858 *Ibid.*, član 41. stav 5.
859 *Ibid.*, član 41. stav 5.
860 *Ibid.*, član 42. stav 1.
861 *Ibid.*, član 42. stav 2.
862 Uredba o sistemu ŠIS II, član 41. stav 1. i Odluka o sistemu ŠIS II, član 58.
863 ESLJP, *Dalea protiv Francuske*, br. 964/07, 2. februara 2010.

Podnosilac predstavke je neuspešno tražio pristup i ispravljanje ili brisanje podataka pred francuskom Komisijom za zaštitu podataka i, konačno, pred Državnim savetom. ESLJP je smatrao da je prijava podnosioca predstavke Šengenskom informacionom sistemu bila u skladu sa zakonom i legitimnom svrhom zaštite nacionalne bezbednosti. Budući da podnosilac predstavke nije pokazao kako je zapravo bio oštećen uskraćivanjem ulaska u Šengenski prostor i budući da su se primenjivale odgovarajuće mere kojima je bio zaštićen od proizvoljnih odluka, mešanje u njegovo pravo na poštovanje privatnog života bilo je srazmerno. Stoga je podnosiočeva predstavka na osnovu člana 8. proglašena neprihvatljivom.

Nadležno domaće nadzorno telo u svakoj državi članici nadgleda nacionalni sistem N-ŠIS. Domaće nadzorno telo mora da obezbedi da se revizija postupaka obrade podataka u sklopu nacionalnog sistema N-ŠIS vrši barem jednom svake četiri godine[864]. Domaćaa nadzorna tela i EDPS sarađuju i obezbeđuju koordinisani nadzor sistema N-ŠIS, a EDPS je odgovoran za nadzor sistema C-ŠIS. Radi transparentnosti, svake dve godine Evropskom parlamentu, Savetu i agenciji eu-LISA šalje se zajednički izveštaj o aktivnostima. Koordinaciona grupa za nadzor sistema ŠIS II (KGNS) osnovana je kako bi se obezbedila koordinacija nadzora ŠIS-a i sastaje se do dva puta godišnje. Grupu čine EDPS i predstavnici nadzornih tela država članica koje su uvele ŠIS II, kao i Islanda, Lihtenštajna, Norveške i Švajcarske, budući da se ŠIS primenjuje i na njih jer su članice Šengenskog sistema[865]. Kipar, Hrvatska i Irska još nisu članovi sistema ŠIS II i zato u KGNS-u učestvuju samo kao posmatrači. U kontekstu KGNS-a, EDPS i domaća nadzorna tela aktivno sarađuju tako što razmenjuju informacije, pomažu međusobno prilikom vršenja revizija i inspekcija, izrađuju nacrte usklađenih predloga za zajednička rešenja svih poteškoća i promovišu svest o pravima na zaštitu podataka[866]. Koordinaciona grupa za nadzor za sistema ŠIS II takođe donosi smernice kao pomoć ispitanicima. Jedan od primera je vodič koji pomaže ispitanicima u ostvarivanju prava na pristup[867].

864 Uredba o sistemu ŠIS II, član 60. stav 2.

865 Videti internet stranicu o Šengenskom informacionom sistemu Evropskog nadzornika za zaštitu podataka (dostupnu na engleskom jeziku).

866 Uredba o sistemu ŠIS II, član 46. i Odluka o sistemu ŠIS II, član 62.

867 Videti SCG za sistem ŠIS II, *The Schengen Information System. A guide for exercising the right of access* (Šengenski informacioni sistem – Vodič za ostvarivanje prava pristupa), dostupan na engleskom jeziku na internet stranici EDPS-a.

Mogućnosti

Evropska komisija sprovela je 2016. postupak ocenjivanja sistema ŠIS[868] koji je pokazao da su uspostavljeni domaći mehanizmi koji ispitanicima omogućavaju pristup sopstvenim ličnim podacima, kao i njihovu ispravku i brisanje u sistemu ŠIS II ili ostvarenje naknade u vezi sa netačnim podacima. Kako bi se poboljšala delotvornost sistema SIS II, Evropska komisija iznela je tri predloga o uredbama:

- Uredba o uspostavi, delovanju i korišćenju sistema ŠIS u oblasti graničnih kontrola, kojom bi se stavila van snage Uredba o sistemu ŠIS II,

- Uredba o uspostavi, delovanju i korišćenju sistema ŠIS u oblasti saradnje policije i pravosudnih tela u krivičnim predmetima, kojom bi se, između ostalog, van snage stavila Odluka o sistemu ŠIS II i

- Uredba o upotrebi sistema ŠIS za povratak državljana trećih zemalja koji nezakonito borave na nekom području.

Važno je napomenuti da se predlozima omogućava obrada drugih kategorija biometrijskih podataka osim fotografija i otisaka prstiju, koji su već uključeni u postojeći sistem ŠIS II. Prikazi lica, otisci dlana i DNK profili takođe će se čuvati u bazi podataka ŠIS. Osim toga, Uredbom o sistemu ŠIS II i Odlukom o sistemu ŠIS II dozvoljena je mogućnost pretraživanja otisaka prstiju radi identifikacije pojedinca, dok je predlozima ta pretraga učinjena obaveznom ako se identitet osobe ne može utvrditi na drugi način. Prikazi lica, fotografije i otisci dlanova primenjivće se za pretraživanje sistema i identifikaciju lica kada to postane tehnički izvodljivo. Nova pravila o biometrijskim karakteristikama uzrokuju posebne rizike za prava pojedinaca. U mišljenju o predlozima Komisije[869] EDPS je istakao da su biometrijski podaci izuzetno osetljivi i da njihovo uvođenje u tako opsežnu bazu podataka treba da se zasniva na proceni potrebe za njihovim uvršćivanjem u ŠIS koja će se zasnivati na dokazima. Drugim rečima, potrebno je dokazati potrebu za obradom tih novih karakteristika. EDPS je takođe zaključio da je potrebno dodatno pojasniti koja se vrsta podataka može uvrstiti u DNK profil. Budući da DNK profil može da sadrži osetljive podatke

868 Evropska komisija (2016), Izveštaj Komisije Evropskom parlamentu i Savetu o oceni druge generacije Šengenskog informacionog sistema (ŠIS II) u skladu s članom 24. stav 5., članom 43. stav 3. i članom 50. stav 5. Uredbe (EZ) br. 1987/2006 kao i članom 59. stav 3. i članom 66. stav 5. Odluke 2007/533/PUP, COM(2016) 880 final, Bruxelles, 21. decembra 2016.

869 EDPS (2017.), Mišljenje Evropskog nadzornika za zaštitu podataka o novoj pravnoj osnovi Šengenskog informacionog sistema, Mišljenje 7/2017, 2. maja 2017.

(najbolji primer bi bili podaci koji otkrivaju zdravstvene probleme), DNK profili koji se čuvaju u ŠIS-u treba da sadrže: „samo najmanju količinu informacija koja je strogo nužna za identifikaciju nestalih osoba i koja ne sadrži izričite zdravstvene podatke, rasno poreklo i druge osetljive podatke"[870]. Međutim, predlozima se uspostavljaju dodatne zaštitne mere kojima se ograničavaju prikupljanje i dalja obrada podataka na ono što je strogo nužno i operativno se zahteva, a pristup se ograničava na osobe koje imaju operativnu potrebu za obradom ličnih podataka[871]. Predlozima se takođe ovlašćuje agencija eu-LISA da redovno izrađuje izveštaje o kvalitetu podataka za države članice, kako bi se redovno preispitivala upozorenja i obezbedio kvalitet podataka[872].

Vizni informacioni sistem

Vizni informacioni sistem (VIS), kojim takođe upravlja eu-LISA, razvijen je kao podrška vršenju zajedničke vizne politike Evropske unije[873]. Zahvaljujući sistemu VIS, države Šengenskog prostora mogu da razmenjuju podatke o podnosiocima zahteva za vizu putem potpuno centralizovanog sistema koji povezuje konzulate i ambasade šengenskih država u državama izvan Evropske unije sa spoljašnjim graničnim prelazima svih šengenskih država. U VIS-u se obrađuju podaci u vezi sa zahtevima za vizama za kratkotrajni boravak ili za prolazom kroz Šengenski prostor. Uz pomoć biometrijskih podataka, a najviše otisaka prstiju, sistem VIS pograničnim organima omogućava da provere da li je osoba koja je pokazala vizu njen važeći nosilac, kao i da identifikuju osobe bez ikakvih dokumenata ili sa lažnim dokumentima.

Uredbom (EZ) br. 767/2008 Evropskog parlamenta i Saveta o viznom informacionom sistemu (VIS) i razmeni podataka među državama članicama o vizama za kratkotrajni boravak (Uredbom o VIS-u) utvrđuju se uslovi i postupci za prenos ličnih poda-

870 *Ibid*., stav 22.

871 Evropska komisija (2016), Predlog uredbe Evropskog parlamenta i Saveta o uspostavi, radu i upotrebi Šengenskog informacionog sistema (ŠIS) u oblasti policijske saradnje i pravosudne saradnje u krivičnim stvarima, izmeni Uredbe (EU) br. 515/2014 i stavljanju van snage Uredbe (EZ) br. 1986/2006, Odluke Saveta 2007/533/PUP i Odluke Komisije 2010/261/EU, COM(2016) 883 final, Bruxelles, 21. decembra 2016.

872 *Ibid*., str. 15.

873 Savet Evropske unije (2004), Odluka Saveta 2004/512/EZ od 8. juna 2004. o uspostavi viznog informacionog sistema (VIS), SL 2004 L 213; Uredba (EZ) br. 767/2008 Evropskog parlamenta i Saveta od 9. jula 2008. o viznom informacionom sistemu (VIS) i razmeni podataka među državama članicama o vizama za kratkotrajni boravak, SL 2008 L 218 (Uredba o VIS-u); Savet Evropske unije (2008), Odluka Saveta 2008/633/PUP od 23. juna 2008. o pristupu određenih tela država članica i Europola viznom informacionom sistemu (VIS) za traženje podataka u svrhu sprečavanja, otkrivanja i istraga terorističkih krivičnih dela i ostalih teških krivičnih dela, SL 2008 L 218.

taka o prijavama za vize za kratkotrajni boravak. Njome se takođe uređuju odluke koje se donose na zahteve, uključujući odluke o poništavanju, oduzimanju ili produženju vize[874]. Uredba o VIS-u uglavnom obuhvata podatke o podnosiocu zahteva, njegove vize, fotografije, otiske prstiju, veze sa prethodnim zahtevima i dokumentaciju o zahtevima osoba koje su u njegovoj pratnji ili podatke o osobama koje su uputile poziv[875]. Pristup VIS-u radi unosa, izmene ili brisanja podataka ograničen je isključivo na organe nadležne za izdavanje viza, dok je pristup radi uvida u podatke obezbeđen organima nadležnim za izdavanje viza i onima nadležnim za kontrole na spoljašnjim graničnim prelazima, imigracione kontrole i azil.

U određenim uslovima domaći nadležni policijski organi i Europol mogu zatražiti pristup podacima unesenima u sistem VIS radi sprečavanja, otkrivanja i istrage terorističkih i krivičnih dela[876]. Budući da je VIS osmišljen kao instrument za pomoć u sprovođenju zajedničke politike o vizama, kada bi se on pretvorio u alat za održavanje javnog reda i mira, prekršilo bi se načelo ograničenja svrhe prema kojem se, kako je objašnjeno u poglavlju 3.2, zahteva da se lični podaci obrađuju isključivo u posebne, izričite i zakonite svrhe i da budu primereni, relevantni i neprekomerni u odnosu na svrhe zbog kojih se obrađuju. Zbog toga domaćim organima za održavanje javnog reda i mira i Europolu nije dozvoljen rutinski pristup bazi podataka VIS. Pristup se može odobriti isključivo za pojedinačne slučajeve i mora biti propraćen strogim zaštitnim merama. Uslovi i zaštitne mere za pristup i uvid tih organa u VIS uređeni su Odlukom Saveta 2008/633/PUP[877].

Uredbom o VIS-u utvrđuju se i prava ispitanika. Ta prava su sledeća:

- pravo na dobijanje informacija od nadležne države članice o identitetu i kontakt podacima rukovaoca podacima koji je zadužen za obradu ličnih podataka u toj državi članici, svrhama zbog kojih se podaci obrađuju unutar VIS-a, kategorijama lica kojima se podaci mogu prenositi (primaocima), kao i o rokovima čuvanja podataka. Podnosioci zahteva za vizu takođe moraju da budu obavešteni o tome da je prikupljanje njihovih ličnih podataka za VIS obavezno za preispitivanje njihovog zahteva, a države članice moraju da ih obaveste i o postojanju prava na

874 Uredba o VIS-u, član 1.

875 Član 5. Uredbe (EZ) br. 767/2008 Evropskog parlamenta i Saveta od 9. jula 2008. o viznom informacionom sistemu (VIS) i razmeni podataka među državama članicama o vizama za kratkotrajni boravak (Uredba o VIS-u), SL 2008 L 218.

876 Savet Evropske unije (2008), Odluka Saveta 2008/633/PUP od 23. juna 2008. o pristupu određenih tela država članica i Europola viznom informacionom sistemu (VIS) za traženje podataka u svrhu sprečavanja, otkrivanja i istraga terorističkih krivičnih dela i ostalih teških krivičnih dela, SL 2008 L 218.

877 *Ibid*.

pristup sopstvenim podacima i prava da se zatraži njihovo ispravljanje ili brisanje, i o postupcima putem kojih mogu ostvariti ta prava[878],

- pravo na pristup ličnim podacima koji se odnose na njih, a koji su zabeleženi u VIS-u[879],
- pravo na ispravku netačnih podataka[880],
- pravo na brisanje nezakonito sačuvanih podataka[881].

Da bi se obezbedio nadzor sistema VIS, osnovana je Koordinaciona grupa za nadzor (KGN) sistema VIS. Čine je predstavnici EDPS-a i domaćih nadzornih tela koji se sastaju dva puta godišnje. Grupu čine predstavnici 28 država članica EU i Islanda, Lihtenštajna, Norveške i Švajcarske.

Eurodak/Eurodac

Eurodak (Eurodac) je skraćenica za Evropski daktiloskopski sistem[882]. Radi se o centralizovanom sistemu sa podacima o otiscima prstiju državljana trećih zemalja i lica bez državljanstva koja traže azil u jednoj od država članica Evropske unije[883]. Sistem se upotrebljava od januara 2003. godine, kada je donesena Uredba Saveta br. 2725/2000, čija je izmena stupila na snagu 2015. Njegova svrha je prvenstveno da pomaže prilikom utvrđivanja koja bi država članica trebalo da bude odgovorna za razmatranje određenog zahteva za azil prema Uredbi Saveta (EZ) br. 604/2013. Tom

878 Uredba o VIS-u, član 37.

879 *Ibid*., član 38. stav 1.

880 *Ibid*., član 38. stav 2.

881 *Ibid*., član 38. stav 2.

882 Videti internet stranicu o Eurodacu Evropskog nadzornika za zaštitu podataka (dostupnu na engleskom jeziku).

883 Uredba Saveta (EZ) br. 2725/2000 od 11. decembra 2000. o osnivanju sistema „Eurodac" za poređenje otisaka prstiju za efikasnu primenu Dablinske konvencije, SL 2000 L 316; Uredba Saveta (EZ) br. 407/2002 od 28. februara 2002. o utvrđivanju određenih pravila za sprovođenje Uredbe (EZ) br. 2725/2000 o osnivanju sistema „Eurodac" za poređenje otisaka prstiju za efikasnu primenu Dablinske konvencije, SL 2002 L 62 (Uredbe o Eurodaku), Uredba (EU) br. 603/2013 Evropskog parlamenta i Saveta od 26. juna 2013. o uspostavi sistema „Eurodac" za poređenje otisaka prstiju za efikasnu primenu Uredbe (EU) br. 604/2013 o utvrđivanju kriterijuma i mehanizama za određivanje države članice odgovorne za razmatranje zahteva za međunarodnu zaštitu koji je u jednoj od država članica podneo državljanin treće zemlje ili osoba bez državljanstva i o zahtevima za poređenje s podacima iz Eurodaca od strane tela krivičnog gonjenja država članica i Europola u svrhu krivičnog gonjenja i o izmeni Uredbe (EU) br. 1077/2011 o osnivanju Evropske agencije za operativno upravljanje opsežnim informacionim sistemima u oblasti slobode, bezbednosti i pravde, SL 2013 L 180, str. 1 (izmenjena Uredba o Eurodaku).

Uredbom se utvrđuju merila i mehanizmi za određivanje države članice odgovorne za razmatranje zahteva za međunarodnu zaštitu koji je u jednoj od država članica podneo državljanin treće zemlje ili lice bez državljanstva (Uredba Dablin III)[884]. Lični podaci u Eurodaku uglavnom služe omogućivanju primene Uredbe Dablin III[885].

Domaća tela nadležna za održavanje javnog reda i mira i Europol smeju da upoređuju otiske prstiju koji se povezuju sa krivičnim istragama s otiscima prstiju u Eurodaku, ali samo u svrhu sprečavanja, otkrivanja ili istrage terorističkih i drugih teških krivičnih dela. Budući da je Eurodac osmišljen kao instrument za pružanje pomoći u vršenju politike EU o azilu, a ne kao alat za održavanje javnog reda i mira, tela nadležna za održavanje javnog reda i mira imaju pravo pristupa bazi podataka samo u određenim slučajevima, u određenim okolnostima i pod određenim uslovima[886]. Za dalju upotrebu podataka u svrhu održavanja javnog reda i mira primenjuje se Direktiva o zaštiti podataka za policiju i tela krivičnog pravosuđa, a podaci koji se upotrebljavaju u osnovnu svrhu pomaganja u sprovođenju Uredbe Dablin III zaštićeni su Opštom uredbom o zaštiti podataka. Zabranjen je dalji prenos ličnih podataka koje prikupi država članica ili Europol u skladu s izmenjenom Uredbom o Eurodaku bilo kojoj trećoj zemlji, međunarodnoj organizaciji ili privatnom subjektu sa sedištem u EU ili izvan nje[887].

Sistem Eurodak sastoji se od centralne jedinice, kojom upravlja eu-LISA, za čuvanje i upoređivanje otisaka prstiju i sistema za elektronski prenos podataka među državama članicama i centralnom bazom podataka. Države članice uzimaju i prenose otiske prstiju svake osobe u uzrastu od najmanje 14 godina koja zatraži azil na njihovom državnom području, kao i svake osobe koja nije državljanin Evropske unije ili osobe bez državljanstva u uzrastu od najmanje 14 godina koja je uhapšena zbog neovlašćenog prelaska njihove spoljašnje granice. Države članice takođe mogu uzeti i preneti otiske prstiju osoba koje nisu državljani Evropske unije ili osoba bez državljanstva koje borave unutar njihovog državnog područja bez dozvole.

Iako države članice mogu pristupiti Eurodaku i zatražiti poređenja sa podacima o otiscima prstiju, samo ona država članica koja je prikupila te otiske i prenela ih cen-

884 Uredba (EU) br. 604/2013 Evropskog parlamenta i Saveta od 26. juna 2013. o utvrđivanju kriterijuma i mehanizama za određivanje države članice odgovorne za razmatranje zahteva za međunarodnu zaštitu koji je u jednoj od država članica podneo državljanin treće zemlje ili osoba bez državljanstva, SL 2013 L 180 (Uredba Dablin III).

885 Izmenjena Uredba o Eurodacu, SL 2013 L 180, str. 1, član 1. stav 1.

886 *Ibid.*, član 1. stav 2.

887 *Ibid.*, član 35.

tralnoj jedinici ima pravo da izmeni podatke ispravljanjem, dopunom ili brisanjem tih podataka[888]. Agencija eu-LISA vodi evidenciju o svim aktivnostima obrade podataka radi praćenja zaštite podataka i obezbeđenja njihove sigurnosti[889]. Domaćaa nadzorna tela pomažu ispitanicima i savetuju ih o ostvarivanju njihovih prava[890]. Prikupljanje i prenos podataka o otiscima prstiju podležu sudskom preispitivanju domaćih sudova[891]. Uredba o zaštiti podataka u institucijama Evropske unije[892] i nadzor EDPS-a primenjuju se na aktivnosti obrade centralnog sistema, kojim upravlja eu-LISA u pogledu Eurodaka[893]. Ako je osoba pretrpela štetu zbog nezakonitog postupka obrade ili drugog delovanja koje nije u skladu s Uredbom o Eurodaku, ima pravo da dobije naknadu štete od države članice odgovorne za pretrpljenu štetu[894]. Međutim, valja napomenuti kako su tražioci azila posebno osetljiva grupa ljudi koji često prelaze dug i opasan put. Zbog njihove osetljivosti i neizvesne situacije u kojoj se često nalaze tokom postupka preispitivanja njihovog zahteva za azil, ostvarenje njihovih prava, uključujući pravo na naknadu štete, u praksi može biti otežano.

Da bi se Eurodak upotrebljavao u svrhe održavanja javnog reda i mira, države članice moraju imenovati tela koja će imati pravo da zatraže pristup Eurodaku kao i tela koja će proveravati da li su zahtevi za upoređivanje zakoniti[895]. Pristup domaćih tela i Europola podacima o otiscima prstiju iz Eurodaka podležu vrlo strogim uslovima. Telo koje upućuje zahtev mora podneti obrazloženi elektronski zahtev tek posle upoređivanja podataka sa podacima iz drugih dostupnih informacionih sistema, kao što su domaće baze podataka o otiscima prstiju i VIS. Mora postojati prevladavajući rizik za javnu bezbednost koji upoređivanje čini srazmernim. Upoređivanje mora biti zaista nužno, mora se odnositi na određeni slučaj i moraju postojati opravdani razlozi za verovanje da bi to upoređivanje značajno doprinelo sprečavanju, otkrivanju ili istrazi bilo kojih krivičnih dela o kojima je reč, naročito kada postoji potkrepljena sumnja da osumnjičeni, učinilac krivičnog dela ili žrtva terorističkog krivičnog dela ili drugog teškog krivičnog dela pripada kategoriji koja podleže prikupljanju

888 *Ibid.*, član 27.

889 *Ibid.*, član 28.

890 *Ibid.*, član 29.

891 *Ibid.*, član 29.

892 Uredba (EZ) br. 45/2001 Evropskog parlamenta i Saveta od 18. decembra 2000. o zaštiti pojedinaca u vezi s obradom ličnih podataka u institucijama i telima Zajednice i o slobodnom kretanju takvih podataka, SL 2001 L 8.

893 Izmenjena Uredba o Eurodacu, SL 2013 L 180, str. 1, član 31.

894 *Ibid.*, član 37.

895 Roots, L. (2015.), „The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination" (Nova Uredba o EURODAC-u: otisci prstiju kao izvor neformalne diskriminacije), *Baltic Journal of European Studies Tallinn University of Technology*, sv. 5, br. 2, str. 108.–129.

otisaka prstiju u sklopu sistema Eurodak. Upoređivanje se mora izvršiti isključivo nad podacima o otiscima prstiju. Europol takođe mora dobiti odobrenje države članice koja je te podatke o otiscima prstiju prikupila.

Lični podaci sačuvani u sistemu Eurodak koji se odnose na tražioce azila čuvaju se 10 godina od datuma uzimanja otisaka prstiju, osim ako ispitanik dobije državljanstvo neke države članice Evropske unije. U tom slučaju se podaci moraju odmah izbrisati. Podaci koji se odnose na strane državljane uhapšene zbog nezakonitog prelaska spoljašnje granice čuvaju se 18 meseci. Ti podaci se moraju izbrisati čim ispitanik dobije dozvolu boravka, napusti područje Evropske unije ili dobije državljanstvo neke države članice. Podaci o osobama kojima je odobren azil ostaju dostupni tri godine radi upoređivanja u kontekstu sprečavanja, otkrivanja i istrage terorističkih i drugih teških krivičnih dela.

Osim svih država članica EU, na osnovu međunarodnih sporazuma sistemom Eurodak služe se i Island, Norveška, Lihtenštajn i Švajcarska.

Koordinaciona grupa za nadzor (KGN) Eurodaka uspostavljena je kako bi se obezbedio nadzor sistema Eurodak. Čine je predstavnici EDPS-a i domaćih nadzornih tela koji se sastaju dva puta godišnje. Grupu čine predstavnici 28 država članica EU i Islanda, Lihtenštajna, Norveške i Švajcarske[896].

Mogućnosti

U maju 2016. godine Komisija je objavila Predlog nove izmene Uredbe o Eurodaku u okviru reforme kojom se nastojalo da se poboljša funkcionisanje Zajedničkog evropskog sistema azila (ZESA)[897]. Predložena izmena je važna jer će se njome znatno proširiti oblast primene originalne baze podataka Eurodak. Eurodak je prvobitno stvoren radi pružanja pomoći u sprovođenju ZESA davanjem dokaza o otiscima prstiju kako bi se omogućilo određivanje države članice koja je odgovorna za razmatranje zahteva za azil podnesenog u EU. Predloženom izmenom proširiće se opseg baze

896 Vidi internet stranicu o Eurodaku Evropskog nadzornika za zaštitu podataka (dostupnu na engleskom jeziku).

897 Evropska komisija, Predlog uredbe Evropskog parlamenta i Saveta o uspostavi sistema „Eurodac" za upoređivanje otisaka prstiju za efikasnu primenu [Uredbe (EU) br. 604/2013 o utvrđivanju kriterijuma i mehanizama za određivanje države članice odgovorne za razmatranje zahteva za međunarodnu zaštitu koji je u jednoj od država članica podneo državljanin treće zemlje ili osoba bez državljanstva] radi identifikacije državljanina treće zemlje ili osobe bez državljanstva s nezakonitim boravkom i o zahtevima za upoređivanje s podacima iz Eurodaca od strane organa krivičnog gonjenja država članica i Europola u svrhu krivičnog gonjenja (izmena), COM(2016) 272 final, 4. maja 2016.

podataka kako bi se olakšao povratak nezakonitih migranata[898]. Domaća tela imaće uvid u bazu podataka u svrhu otkrivanja državljana trećih zemalja koji nezakonito borave u EU ili koji su nezakonito ušli u EU, kako bi prikupila dokaze koji će državama članicama pomoći da ih vrate u njihove zemlje. Usto, pravnim režimom koji je trenutno na snazi zahtevaju se samo prikupljanje i čuvanje otisaka prstiju, dok se u Predlog uvodi prikupljanje prikaza lica pojedinaca[899], što predstavlja drugu vrstu biometrijskih podataka. Predlogom bi se takođe smanjio minimalni uzrast dece od koje se smeju uzimati biometrijski podaci, na šest[900] umesto 14 godina, što je uzrasna granica prema Uredbi iz 2013. Proširena oblast primene Predloga podrazumeva da će ona predstavljati mešanje u prava na privatnost i zaštitu podataka većeg broja pojedinaca koji bi mogli da budu uvršćeni u bazu podataka. Kao protivteža tom mešanju, Predlogom i izmenama i dopunama koje predlaže Odbor LIBE Evropskog parlamenta[901] nastoje da se ojačaju zahtevi u pogledu zaštite podataka. U vreme izrade ovog priručnika rasprave o predlogu u Parlamentu i Savetu još su bile u toku.

Eurosur

Evropski sistem za nadzor granica (Eurosur)[902] osmišljen je kako bi pojačao kontrolu spoljašnjih granica Šengenske zone otkrivanjem, sprečavanjem i suzbijanjem nezakonite imigracije i prekograničnog kriminala. On služi za poboljšanje razmene informacija i operativne saradnje između domaćih koordinacionih centara i agencije

898 Videti Memorandum s objašnjenjima o predlogu, str. 3.

899 Evropska komisija, Predlog uredbe Evropskog parlamenta i Saveta o uspostavi sistema „Eurodac" za upoređivanje otisaka prstiju za efikasnu primenu [Uredbe (EU) br. 604/2013 o utvrđivanju kriterijuma i mehanizama za određivanje države članice odgovorne za razmatranje zahteva za međunarodnu zaštitu koji je u jednoj od država članica podneo državljanin treće zemlje ili lice bez državljanstva] radi identifikacije državljanina treće zemlje ili lica bez državljanstva s nezakonitim boravkom i o zahtevima za upoređivanje s podacima iz Eurodaka od strane organa krivičnog gonjenja država članica i Europola u svrhu krivičnog gonjenja (izmena), COM(2016) 272 final, 4. maja 2016., član 2 stav 1.

900 *Ibid.*, član 2. stav 2.

901 Evropski parlament, *Izveštaj* o Predlogu uredbe Evropskog parlamenta i Saveta o uspostavi sistema „Eurodac" za upoređivanje otisaka prstiju za efikasnu primenu [Uredbe (EU) br. 604/2013 o utvrđivanju kriterijuma i mehanizama za određivanje države članice odgovorne za razmatranje zahteva za međunarodnu zaštitu koji je u jednoj od država članica podneo državljanin treće zemlje ili lice bez državljanstva] radi identifikovanja državljanina treće zemlje ili osobe bez državljanstva s nezakonitim boravkom i o zahtevima za upoređivanje s podacima iz Eurodaca od strane organa krivičnog gonjenja država članica i Europola u svrhu krivičnog gonjenja (izmena), PE 597.620v03-00, 9. juna 2017.

902 Uredba (EU) br. 1052/2013 Evropskog parlamenta i Saveta od 22. oktobra 2013. o uspostavi Evropskog sistema nadzora granica (EUROSUR), SL 2013 L 295.

Frontex, agencije Evropske unije koja je zadužena za razvijanje i primenu novog koncepta integrisanog upravljanja granicama[903]. Njegovi opšti ciljevi su:

- smanjiti broj nezakonitih migranata koji neotkriveni ulaze u Evropsku uniju,
- smanjiti broj smrti nezakonitih migranata spasavanjem većeg broja ljudi na moru,
- povećati unutrašnju sigurnost EU u celini pomažući u sprečavanju prekograničnog kriminala[904].

Eurosur jepočeo sa radom 2. decembra 2013. godine u svim državama članicama sa spoljašnjim granicama, a 1. decembra 2014. i u ostalima. Uredba se primenjuje na nadzor spoljašnjih kopnenih, morskih i vazdušnih granica država članica. Eurosur razmenjuje i obrađuje lične podatke u vrlo ograničenom opsegu, budući da države članice i Frontex smeju da razmenjuju samo identifikacione brojeve brodova. Eurosur razmenjuje operativne informacije, kao što su lokacije patrola i incidenata, a opšte pravilo je da informacije koje se razmenjuju ne smeju da sadrže lične podatke[905]. U izuzetnim slučajevima u kojima se u okviru Eurosara razmenjuju lični podaci Uredbom je utvrđeno da se primenjuje opšti pravni okvir EU za zaštitu podataka[906].

Eurosur zato osigurava pravo na zaštitu podataka, prvenstveno tako što zahteva da su razmene ličnih podataka u skladu sa kriterijumima i zaštitnim merama koji su uspostavljeni Direktivom o zaštiti podataka za policiju i organe krivičnog pravosuđa i Opštom uredbom o zaštiti podataka[907].

---

903 Uredba (EU) br. 2016/1624 Evropskog parlamenta i Saveta od 14. septembra 2016. o evropskoj graničnoj i obalnoj straži i o izmeni Uredbe (EU) 2016/399 Evropskog parlamenta i Saveta i o stavljanju van snage Uredbe (EZ) br. 863/2007 Evropskog parlamenta i Saveta, Uredbe Saveta (EZ) br. 2007/2004 i Odluke Saveta 2005/267/EZ, SL L 251.

904 Vidi i: Evropska komisija (2008.), Komunikacija Komisije Evropskom parlamentu, Savetu, Evropskom ekonomskom i socijalnom odboru i Odboru regija: Razmatranje uspostave Evropskog sistema za nadzor granica (Eurosur), COM(2008) 68 final, Bruxelles, 13. februara 2008.; Evropska komisija (2011.), Procena efekta uz Predlog uredbe Evropskog parlamenta i Saveta o uspostavi Evropskog sistema za nadzor granica (Eurosur), radni dokument osoblja, SEC(2011) 1536 final, Bruxelles,12. decembra 2011, str. 18.

905 Evropska komisija, *EUROSUR: Protecting the Schengen external borders – protecting migrants' lives. EUROSUR in a nutshell* (EUROSUR: zaštita spoljašnjih granica Šengenske zone – zaštita života migranata), 29. novembra 2013.

906 Uredba 1052/2013, uvodna izjava 13 i član 13.

907 *Ibid*., uvodna izjava 13 i član 13.

Carinski informacioni sistem

Drugi važan informacioni sistem uspostavljen na nivou EU jeste Carinski informacioni sistem (CIS)[908]. Tokom uspostave unutrašnjeg tržišta ukinute su sve kontrole i formalnosti u vezi sa robom koja se kreće unutar područja EU, što je povećalo rizik od prevare. Kao protivteža tom riziku pojačana je saradnja među carinskim upravama država članica. Svrha CIS-a je da pomogne državama članicama u sprečavanju, istrazi i gonjenju teških kršenja carinskih i poljoprivrednih zakona na nivou država i EU. CIS je osnovan dvama pravnim aktima koji su doneseni na različitim pravnim osnovama: Uredba Saveta (EZ) br. 515/97 odnosi se na saradnju različitih domaćih upravnih tela radi suzbijanja prevara u kontekstu carinske unije i zajedničke poljoprivredne politike, a Odlukom Saveta 2009/917/PUP nastoji se da se pomogne u sprečavanju, istrazi i gonjenju teških povreda carinskih zakona. To znači da se CIS ne odnosi samo na održavanje javnog reda i mira.

Informacije iz CIS-a obuhvataju lične podatke koji se odnose na zadržane, oduzete ili zaplenjene proizvode, prevozna sredstva, preduzeća, lica, robu i gotovinu. Kategorije podataka koji se mogu obrađivati jasno su određene, a uključuju imena, državljanstvo, pol, datum i mesto rođenja dotičnih lica, razlog uvrštavanja njihovih podataka u sistem i registracioni broj prevoznog sredstva[909]. Te informacije se mogu upotrebljavati samo u svrhe opažanja, izveštavanja ili izvršavanja određenih inspekcija ili u svrhe strateške ili operativne analize u vezi sa licima osumnjičenim za povrede carinskih propisa.

Pristup CIS-u dozvoljen je domaćim carinskim, poreskim, poljoprivrednim, javno-zdravstvenim i policijskim organima kao i Europolu i Eurodžastu.

Obrada ličnih podataka mora biti u skladu sa posebnim pravilima utvrđenima Uredbom br. 515/97 i Odlukom Saveta 2009/917/PUP, kao i odredbama Opšte uredbe o zaštiti podataka, Uredbe o zaštiti podataka u institucijama Evropske unije, modernizovane Konvencije br. 108 i Preporuke o policiji. EDPS je odgovoran za nadzor usklađenosti CIS-a s Uredbom (EZ) br. 45/2001. Sastaje se barem jednom godišnje

908 Savet Evropske unije (1995.), Akt Saveta od 26. jula 1995. o sastavljanju Konvencije o upotrebi informacione tehnologije u carinske svrhe, SL 1995 C 316, koju je izmenio Savet Evropske unije (2009.), Uredba br. 515/97 od 13. marta 1997. o uzajamnoj pomoći upravnih organa država članica i o saradnji potonjih s Komisijom radi obezbeđenja pravilne primene propisa o carinskim i poljoprivrednim pitanjima, Odluka Saveta 2009/917/PUP od 30. novembra 2009. o upotrebi informacionih tehnologija u carinske svrhe, SL 2009 L 323 (Odluka o CIS-u).

909 Vidi Odluku o CIS-u, članovi 24., 25. i 28.

sa svim domaćim telima za zaštitu podataka koja su nadležna za nadzor u vezi sa CIS-om.

Interoperabilnost informacionih sistema Evropske unije

Upravljanje migracijama, integrisano upravljanje spoljašnjim granicama EU, kao i borba protiv terorizma i prekograničnog kriminala, važni su i sve složeniji izazovi u današnjem globalizovanom svetu. U poslednjih nekoliko godina EU razvija novi sveobuhvatan pristup zaštiti i očuvanju bezbednosti bez dovođenja u pitanje vrednosti i osnovnih sloboda EU. U tim nastojanjima je ključna stvarna razmena informacija među domaćim telima za sprovođenje zakonodavstva i među državama članicama i nadležnim agencijama EU[910]. Postojeći informacioni sistemi EU za upravljanje granicama i unutrašnju bezbednost imaju sopstvene ciljeve, institucionalnu organizaciju, ispitanike i korisnike. EU radi na otklanjanju nedostataka rascepkanog upravljanja podacima u EU među različitim informacionim sistemima kao što su ŠIS II, VIS i Eurodak tako što istražuje mogućnost njihove međusobne saradnje[911]. Glavni cilj je da se obezbedi da nadležni policijski, carinski i pravosudni organi sistemski dobijaju informacije koje su im potrebne za izvršavanje dužnosti i istovremeno održe ravnotežu u pogledu prava na privatnost, zaštitu podataka i druga osnovna prava.

Interoperabilnost/međusobna saradnja je „sposobnost informacionih sistema da razmenjuju podatke i omogućavaju deljenja informacija"[912]. Tom razmenom se ne smeju ugroziti nužna stroga pravila o pristupu i upotrebi koja su garantovana Opštom uredbom o zaštiti podataka, Direktivom o zaštiti podataka za policiju i organe krivičnog pravosuđa i Poveljom EU o osnovnim pravima, kao i svim ostalim relevantnim

910 Evropska komisija (2016), Komunikacija Komisije Evropskom parlamentu i Savetu: Jači i pametniji informacioni sistemi za granice i bezbednost, COM(2016) 205 final, Bruxelles, 6. aprila 2016., Evropska komisija (2016.), Komunikacija Komisije Evropskom parlamentu, Evropskom savetu i Savetu: Povećanje bezbednosti u svetu mobilnosti: bolja razmena informacija u borbi protiv terorizma i jače spoljašnje granice, COM(2016) 602 final, Bruxelles, 14. septembra 2016., Evropska komisija (2016.), Predlog uredbe Evropskog parlamenta i Saveta o upotrebi Šengenskog informacionog sistema za vraćanje državljana trećih zemalja s nezakonitim boravkom. Videti i Komunikaciju Komisije Evropskom parlamentu, Evropskom savetu i Savetu: Sedmi Izveštaj o napretku prema uspostavi efikasne i istinske bezbednosne unije, COM(2017) 261 final, Bruxelles, 16. maja 2017.

911 Savet Evropske unije (2005), Haški program: jačanje slobode, bezbednosti i pravde u Evropskoj uniji, SL 2005 C 53, Evropska komisija (2010), Komunikacija Komisije Evropskom parlamentu i Savetu: Pregled upravljanja informacijama u oblasti slobode, bezbednosti i pravde, COM(2010) 385 final, Europska komisija (2016.), Komunikacija Komisije Europskom parlamentu i Vijeću: Jači i pametniji informacijski sistemi za granice i sigurnost, COM(2016) 205 final, Bruxelles, 6. aprila 2016., Evropska komisija (2016), Odluka Komisije od 17. juna 2016. o osnivanju grupe stručnjaka na visokom nivou za informacione sisteme i interoperabilnost, SL 2016 C 257.

912 Evropska komisija (2016), Komunikacija Komisije Evropskom parlamentu i Savetu: Jači i pametniji informacioni sistemi za granice i bezbednost, COM(2016) 205 final, Bruxelles, 6. aprila 2016., str. 14.

propisima. Integrisana rešenja za upravljanje podacima ne smeju da utiču na načela ograničenja svrhe ili tehničke ili integrisane zaštite podataka[913].

Uz poboljšanje funkcija tri glavna informaciona sistema – sistema ŠIS II, VIS i Eurodak – Komisija je predložila uspostavu četvrtog centralizovanog sistema za upravljanje granicama koji bi obuhvatao državljane trećih zemalja: sistem ulaska/izlaska (SUI)[914], čije se uvođenje planira za 2020.[915] Komisija je takođe izdala predlog o uspostavljanju Evropskog sistema za informacije o putovanjima i njihovom odobrenju (ETIAS/ESIPO)[916], u kojem će se prikupljati informacije o licima koja putuju bez vize u EU, kako bi se omogućile napredne provere u vezi sa nezakonitim migracijama i bezbednosne provere.

913 *Ibid*., str. 4 –5.

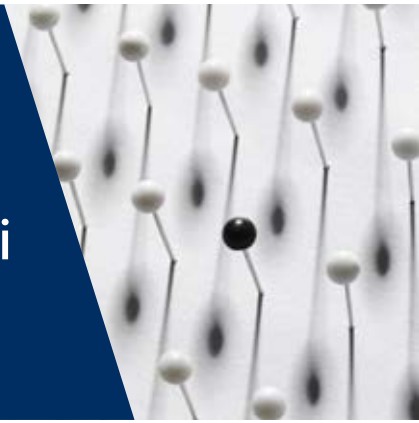
914 Evropska komisija (2016), Predlog uredbe Evropskog parlamenta i Saveta o uspostavi sistema ulaska/izlaska (EES) za registraciju podataka o ulasku i izlasku kao i podataka o zabrani ulaska za državljane trećih zemalja koji prelaze spoljašnje granice država članica Evropske unije i određivanju uslova za pristup EES-u za potrebe krivičnog gonjenja i o izmeni Uredbe (EZ) br. 767/2008 i Uredbe (EZ) br. 1077/2011, COM(2016) 194 final, Bruxelles, 6. aprila 2016.

915 Evropska komisija (2016.), Komunikacija Komisije Evropskom parlamentu i Savetu: Jači i pametniji informacioni sistemi za granice i bezbednost, COM(2016) 205 final, Bruxelles, 6. aprila 2016., str. 5.

916 Evropska komisija (2016.), Predlog uredbe Evropskog parlamenta i Saveta o uspostavi evropskog sistema za informacije o putovanjima i njihovom odobrenju (ETIAS) i izmeni Uredbi (EU) br. 515/2014, (EU) 2016/399, (EU) 2016/794 i (EU) 2016/1624, COM(2016) 731 final, 16. novembra 2016.

9

Posebne vrste podataka i propisi o njihovoj zaštiti



EU	Obuhvaćena pitanja	Savet Evrope
Opšta uredba o zaštiti podataka Direktiva o privatnosti i elektronskim komunikacijama	**Elektronske komunikacije**	Modernizovana Konvencija br. 108 Preporuka o telekomunikacionim uslugama
Opšta uredba o zaštiti podataka, član 89.	**Radni odnosi**	Modernizovana Konvencija br. 108 Preporuka o zaposlenju ESLJP, *Copland protiv Ujedinjenog Kraljevstva*, br. 62617/00, 2007.
Opšta uredba o zaštiti podataka, član 9. stav 2. tačke (h) i (i)	**Medicinski podaci**	Modernizovana Konvencija br. 108 Preporuka o medicinskim podacima ESLJP, *Z protiv Finske*, br. 22009/93, 1997.
Uredba o kliničkim ispitivanjima	**Klinička ispitivanja**	
Opšta uredba o zaštiti podataka, član 6. stav 4. i član 8.	**Statistika**	Modernizovana Konvencija br. 108 Preporuka o statističkim podacima
Uredba (EZ) br. 223/2009 o evropskoj statistici SPEU, C-524/06, *Huber protiv Bundesrepublik Deutschland* [VV], 2008.	**Službena statistika**	Modernizovana Konvencija br. 108 Preporuka o statističkim podacima

EU	Obuhvaćena pitanja	Savet Evrope
Direktiva 2014/65/EU o tržištu finansijskih instrumenata Uredba (EU) br. 648/2012 o OTC izvedenicama, središnjoj drugoj ugovornoj strani i trgovinskom repozitorijumu Uredba (EZ) br. 1060/2009 o agencijama za kreditni rejting Direktiva 2007/64/EZ o platnim uslugama na unutrašnjem tržištu	Finansijski podaci	Modernizovana Konvencija br. 108 Preporuka 90 (19) koja se upotrebljava za plaćanja i druge srodne aktivnosti ESLJP, *Michaud protiv Francuske*, br. 12323/11, 2012.

U nekoliko slučajeva na evropskom nivou su doneseni posebni pravni instrumenti kojima se u određenim situacijama detaljnije primenjuju opšta pravila modernizovane Konvencije br. 108 ili Opšte uredbe o zaštiti podataka.

9.1. Elektronske komunikacije

Ključne tačke

- Posebna pravila o zaštiti podataka u oblasti telekomunikacija, sa posebnim naglaskom na telefonske usluge, sadržana su u Preporuci Saveta Evrope iz 1995. godine.
- Obrada ličnih podataka koji se odnose na pružanje komunikacionih usluga na nivou Evropske unije uređena je Direktivom o privatnosti i elektronskim komunikacijama.
- Poverljivost elektronskih komunikacija odnosi se ne samo na sadržaj komunikacije, već i na metapodatke, kao što su informacije o tome ko je komunicirao sa kim, kad se komunikacija odvijala i koliko dugo je trajala, kao i na podatke o lokaciji, kao što je lokacija sa koje su podaci objavljeni.

U komunikacionim mrežama je veća mogućnost neopravdanog mešanja u ličnu sferu korisnika zbog razvijenih tehničkih mogućnosti prisluškivanja i praćenja komunikacije koja se odvija putem takvih mreža. Zbog toga se smatralo da su potrebni posebni propisi o zaštiti podataka radi otklanjanja određenih rizika kojima su izloženi korisnici komunikacionih usluga.

Savet Evrope usvojio je 1995. godine Preporuku o zaštiti podataka u oblasti telekomunikacija koja se naročito odnosila na telefonske usluge[917]. U skladu sa tom preporukom, svrhe prikupljanja i obrade ličnih podataka u kontekstu telekomunikacija treba ograničiti na: spajanje korisnika na mrežu, ponudu određene telekomunikacione usluge, naplatu, proveru, obezbeđivanje optimalnog tehničkog rada i razvoj mreže i usluge.

Posebna pažnja je posvećena i upotrebi komunikacionih mreža za slanje poruka neposrednog marketinga. Poruke neposrednog marketinga po pravilu ne smeju da budu usmerene ka pretplatniku koji je izričito izjavio da ne želi da ih dobija. Uređaji za automatsko pozivanje koji prenose unapred snimljene reklamne poruke smeju da se upotrebljavaju samo ako je pretplatnik dao svoj izričitu pristanak. Domaćim zakonodavstvom propisuju se detaljna pravila u toj oblasti.

U sklopu **pravnog okvira EU,** posle prvog pokušaja 1997. godine, Direktiva o privatnosti i elektronskim komunikacijama donesena je 2002. i izmenjena 2009. godine. To je učinjeno radi dopunjavanja i prilagođavanja odredbi nekadašnje Direktive o zaštiti podataka telekomunikacionom sektoru[918].

Primena Direktive o privatnosti i elektronskim komunikacijama ograničena je na komunikacione usluge u javnim elektronskim mrežama.

U Direktivi o privatnosti i elektronskim komunikacijama razlikuju se tri glavne kategorije podataka nastalih pri komuniciranju:

- podaci koji čine sadržaj poruka poslatih tokom komunikacije; ti podaci su strogo poverljivi,

- podaci potrebni za uspostavu i održavanje komunikacije, takozvani metapodaci, koji se u Direktivi nazivaju „podaci o saobraćaju", kao što su informacije o osobama koje komuniciraju, vremenu i trajanju komunikacije,

---

917 Savet Evrope, Komitet ministara (1995), Preporuka Rec(95)4 državama članicama o zaštiti ličnih podataka u oblasti telekomunikacionih usluga, sa posebnim naglaskom na telefonske usluge, 7. februara 1995.

918 Direktiva 2002/58/EZ Evropskog parlamenta i Saveta od 12. jula 2002. o obradi ličnih podataka i zaštiti privatnosti u oblasti elektronskih komunikacija, SL 2002 L 201 (Direktiva o privatnosti i elektronskim komunikacijama), kako je izmenjena Direktivom 2009/136/EZ Evropskog parlamenta i Saveta od 25. novembra 2009. o izmeni Direktive 2002/22/EZ o univerzalnim uslugama i pravima korisnika s obzirom na elektronske komunikacione mreže i usluge, Direktive 2002/58/EZ o obradi ličnih podataka i zaštiti privatnosti u sektoru elektronskih komunikacija i Uredbe (EZ) br. 2006/2004 o saradnji između domaći tela odgovornih za sprovođenje zakona o zaštiti potrošača, SL 2009 L 337.

- metapodaci obuhvataju podatke koji se posebno odnose na lokaciju komunikacionog uređaja, takozvane podatke o lokaciji; ti podaci su istovremeno podaci o lokaciji korisnika komunikacionih uređaja, posebno kad je reč o korisnicima mobilnih komunikacionih uređaja.

Podatke o prometu može upotrebljavati pružalac usluge za potrebe naplate usluge i za tehničko pružanje usluge. Međutim, uz pristanak ispitanika, ti podaci se mogu otkriti drugim rukovaocima podacima koji pružaju dodatne usluge, kao što je davanje informacija na osnovu lokacije korisnika: o sledećoj stanici podzemne železnice ili apote ili o vremenskoj prognozi za tu lokaciju.

Prema članu 15. Direktive o privatnosti i elektronskim komunikacijama, ostali pristupi podacima o komunikacijama u elektronskim mrežama moraju ispunjavati zahteve za opravdano mešanje u pravo na zaštitu podataka kako je utvrđeno u članu 8. stav 2. EKLJP-a i potvrđeno u članovima 8. i 52. Povelje EU o osnovnim pravima. Takav pristup može uključivati pristup u svrhu istraga krivičnih dela.

Izmenama Direktive o privatnosti i elektronskim komunikacijama iz 2009. godine[919] uvedeno je sledeće:

- Ograničenja za slanje e-pošte u svrhu neposrednog marketinga proširena su na usluge kratkih (SMS) poruka, usluge multimedijskih poruka i ostale vrste sličnih aplikacija. Reklamna e-pošta zabranjena je, osim uz prethodni pristanak. Bez takvog pristanka dozvoljeno je obraćanje reklamnom e-poštom samo pređašnjim kupcima ako su dali svoje adrese e-pošte i nemaju primedbi na to.

- Državama članicama nametnuta je obaveza omogućavanja pravnih lekova protiv kršenja zabrane neželjene komunikacije[920].

- Postavljanje kolačića, softvera koji nadgleda i beleži aktivnosti korisnika računara, više nije dozvoljeno bez pristanka korisnika računara. Domaćim zakono-

919 Direktiva 2009/136/EZ Evropskog parlamenta i Saveta od 25. novembra 2009. o izmeni Direktive 2002/22/EZ o univerzalnim uslugama i pravima korisnika s obzirom na elektronske komunikacione mreže i usluge, Direktive 2002/58/EZ o obradi ličnih podataka i zaštiti privatnosti u sektoru elektronskih komunikacija i Uredbe (EZ) br. 2006/2004 o saradnji između domaćihih tela odgovornih za sprovođenje zakona o zaštiti potrošača, SL 2009 L 337.

920 Vidi izmenjenu Direktivu, član 13.

davstvom treba detaljnije urediti način na koji treba izraziti i dobiti pristanak radi obezbeđenja odgovarajuće zaštite[921].

Ako dođe do povrede podataka zbog neovlašćenog pristupa, gubitka ili uništavanja podataka, o tome je potrebno odmah obavestiti nadležno nadzorno telo. Pretplatnike je potrebno obavestiti ako je šteta koju su eventualno pretrpeli posledica povrede podataka[922].

Prema Direktivi o zadržavanju podataka[923] pružaoci komunikacionih usluga bili su dužni da zadržavaju metapodatke. Međutim, SPEU je tu direktivu proglasio nevažećom (za više pojedinosti vidi deo 8.3).

Mogućnosti

U januaru 2017. godine Evropska komisija usvojila je novi predlog Uredbe o e-privatnosti koja bi zamenila nekadašnju Direktivu o privatnosti i elektronskim komunikacijama. Glavni cilj i dalje bi bila zaštita „osnovnih prava i sloboda fizičkih i pravnih lica pri davanju i upotrebi elektronskih komunikacionih usluga, posebno prava na poštovanje privatnog života i komuniciranja i zaštita fizičkih lica u pogledu obrade ličnih podataka". Novim predlogom istovremeno bi se obezbedilo slobodno kretanje elektronskih komunikacionih podataka i elektronskih komunikacionih usluga unutar Unije[924]. Dok se Opštom uredbom o zaštiti podataka prvenstveno upućuje na član 8. Povelje EU o osnovnim pravima, predloženom Uredbom nastoji se da se ugradi član 7. Povelje u sekundarno pravo Unije.

Uredbom bi se odredbe prethodne Direktive prilagodile novim tehnologijama i tržištu tako da bi se izgradio sveobuhvatan i dosledan okvir u sklopu Opšte uredbe o zaštiti podataka. U tom smislu, Uredba o e-privatnosti bila bi *lex specialis* za Opštu uredbu o zaštiti podataka, kojim bi se ona prilagodila elektronskim komunikacionim podacima koji čine lične podatke. Novom Uredbom obuhvata se obrada „elek-

921 Vidi *Ibid.*, član 5.; vidi i Radna grupa iz člana 29. (2012.), *Mišljenje 04/2012 o izuzeću od obaveze davanja pristanka za postavljanje kolačića*, WP 194, Bruxelles, 7. juna 2012.

922 Vidi i Radna grupa iz člana 29. (2011), Radni dokument 01/2011 o trenutnom okviru Evropske unije za povredu ličnih podataka i preporukama za budući razvoj politike, WP 184, Bruxelles, 5. aprila 2011.

923 Direktiva 2006/24/EZ Evropskog parlamenta i Saveta od 15. marta 2006. o zadržavanju podataka dobijenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacionih usluga ili javnih komunikacionih mreža i o izmeni Direktive 2002/58/EZ, SL 2006 L 105.

924 Predlog uredbe Evropskog parlamenta i Saveta o poštovanju privatnog života i zaštiti ličnih podataka u elektronskim komunikacijama i stavljanju van snage Direktive 2002/58/EZ (Uredba o privatnosti i elektronskim komunikacijama) (COM(2017) 10 final), član 1.

tronskih komunikacionih podataka", uključujući sadržaj elektronskih komunikacija i metapodatke koji nisu nužno lični podaci. Njeno područje primene ograničeno je na EU, uključujući slučajeve u kojima se podaci prikupljeni u EU obrađuju izvan EU, a proširuje se na pružaoce komunikacionih usluga OTT (engl. *Over The Top*). To su pružaoci usluga koji isporučuju sadržaj, usluge ili aplikacije putem interneta, bez neposrednog uključivanja mrežnog operatera ili pružaoca usluga interneta (ISP). Primeri takvih pružalaca usluga uključuju Skype (glasovni i video-pozivi), WhatsApp (razmena poruka), Google (pretraživanje), Spotify (muzika) i Netflix (video-sadržaj). Mehanizmi izvršenja Opšte uredbe o zaštiti podataka primenjivali bi se i na novu Uredbu.

Donošenje Uredbe o e-privatnosti predviđeno je pre 25. maja 2018. godine, kada Opšta uredba o zaštiti podataka stupa na snagu za svih 28 država članica. Međutim, to zavisi od odobrenja i Evropskog parlamenta i Saveta[925].

9.2. Podaci o radu

Ključne tačke

- Posebna pravila o zaštiti podataka u okviru radnih odnosa sadržana su u Preporuci o podacima o zaposlenju Saveta Evrope.
- U Opštoj uredbi o zaštiti podataka radni odnosi spominju se konkretno samo u kontekstu obrade osetljivih podataka.
- Valjanost pristanka, koji mora biti dat dobrovoljno, kao pravne osnove za obradu podataka o zaposlenima može biti sumnjiva s obzirom na ekonomsku neravnotežu između poslodavca i zaposlenog. Okolnosti davanja pristanka moraju se pažljivo proceniti.

Obrada podataka u kontekstu radnih odnosa podleže opštem zakonodavstvu EU koje se odnosi na zaštitu ličnih podataka. Međutim, jedna uredba[926] se posebno odnosi na zaštitu obrade ličnih podataka u evropskim institucijama u kontekstu rada (između ostalog). U Opštoj uredbi o zaštiti podataka radni odnosi posebno se

925 Za više informacija vidi Evropska komisija (2017), „Komisija predlaže pravila o visokom nivou zaštite privatnosti za sve elektronske komunikacije i ažurira pravila o zaštiti podataka za institucije EU", saopštenje za medije, 10. januara 2017.

926 Uredba (EZ) br. 45/2001 Evropskog parlamenta i Saveta od 18. decembra 2000. o zaštiti pojedinaca u vezi s obradom ličnih podataka u institucijama i telima Zajednice i o slobodnom kretanju takvih podataka, SL 2001 L 8.

spominju u članu 9. stavu 2., kojim se utvrđuje da se lični podaci mogu obrađivati prilikom izvršavanja obaveza ili ostvarivanja posebnih prava rukovaoca podacima ili ispitanika u oblasti rada.

Prema Opštoj uredbi o zaštiti podataka, zaposleni bi trebalo da imaju mogućnost da jasno razlikuju podatke za čiju su obradu/čuvanje dali dobrovoljnu pristanak i svrhe u koje se njihovi podaci čuvaju. Zaposleni takođe treba da budu informisani o svojim pravima i periodu čuvanja podataka pre nego što daju pristanak. Ako postoji verovatnoća da bi povreda ličnih podataka dovela do visokog rizika u pogledu prava i sloboda pojedinaca, poslodavac mora o toj povredi da obavesti zaposlenog. Članom 88. Uredbe državama članicama se dozvoljava da utvrde preciznija pravila sa ciljem obezbeđivanja zaštite prava i sloboda zaposlenih u vezi s obradom njihovih ličnih podataka u kontekstu rada.

Primer: U predmetu *Worten*[927] podaci su uključivali zapis o radnom vremenu koji je sadržao periode rada i odmora u danu, što predstavlja lične podatke. Domaćim zakonodavstvom se može obavezati poslodavac da zapise o radnom vremenu stavi na raspolaganje domaćim organima nadležnim za nadgledanje uslova rada. Time bi se omogućio neposredan pristup odgovarajućim ličnim podacima. Međutim, pristup ličnim podacima je nužan kako bi se domaćem telu omogućio nadzor zakonodavstva u vezi sa uslovima rada[928].

Što se tiče **Saveta Evrope**, Preporuka o podacima o radu izdata je 1989. i revidirana 2015. godine[929] Preporuka obuhvata obradu ličnih podataka u svrhe rada u privatnom i javnom sektoru. Obrada mora biti u skladu s određenim načelima i ograničenjima, poput načela transparentnosti i savetovanja sa predstavnicima zaposlenih pre uvođenja nadzornih sistema na radnom mestu. U Preporuci se takođe navodi da poslodavci treba da primenjuju preventivne mere, poput filtera, umesto nadgledanja upotrebe interneta zaposlenih.

927 SPEU, C-342/12, *Worten – Equipamentos para o Lar, SA protiv Autoridade para as Condições de Trabalho (ACT)*, 30. maja 2013, stav 19.

928 *Ibid*., stav 43.

929 Savet Evrope, Komitet ministara (2015.), Preporuka Rec(2015)5 državama članicama o obradi ličnih podataka u kontekstu zapošljavanja, april 2015.

Pregled najčešćih problema u vezi sa zaštitom podataka u kontekstu rada nalazi se u radnom dokumentu Radne grupe iz člana 29.[930] Radna grupa analizirala je važnost pristanka kao pravne osnove za obradu podataka o zaposlenosti[931]. Utvrdila je da će zbog ekonomske neravnoteže između poslodavca koji traži pristanak i zaposlenog koji daje pristanak uvek biti sumnjivo da li je pristanak dat dobrovoljno. Zato pri proceni valjanosti pristanka u kontekstu rada treba pažljivo razmotriti okolnosti u kojima se pristanak upotrebljava kao pravna osnova za obradu podataka.

Čest problem u vezi sa zaštitom podataka u današnjem tipičnom radnom okruženju jeste opseg legitimnog nadzora elektronskih komunikacija zaposlenih na radnom mestu. Često se tvrdi da se taj problem može lako rešiti zabranom privatne upotrebe komunikacionih sredstava na radnom mestu. Međutim, takva opšta zabrana bi mogla da bude nesrazmerna i nerealna. Presude ESLJP-a u predmetima *Copland protiv Ujedinjenog Kraljevstva* i *Bărbulescu protiv Rumunije* posebno su važne u tom kontekstu.

Primer: U predmetu *Copland protiv Ujedinjenog Kraljevstva* [932] tajno je nadgledana upotreba telefona, e-pošte i interneta zaposlene u višoj školi kako bi se utvrdilo da li prekomerno upotrebljava školska sredstva u lične svrhe. ESLJP je smatrao da su telefonski pozivi iz poslovnih prostorija obuhvaćeni pojmovima privatnog života i dopisivanja. Stoga su takvi pozivi i e-pošta upućeni sa radnog mesta, kao i informacije dobijene na osnovu nadzora lične upotrebe interneta, zaštićeni članom 8. EKLJP-a. U slučaju podnositeljke predstavke nisu postojale odredbe kojima se uređuju okolnosti u kojima poslodavci mogu da nadgledaju upotrebu telefona, e-pošte i interneta zaposlenog. Zato mešanje nije bilo u skladu sa zakonom. ESLJP je stoga zaključio da je došlo do povrede člana 8. Konvencije.

Primer: U predmetu *Bărbulescu protiv Rumunije*[933] podnosilac predstavke je bio otpušten zbog upotrebe interneta tokom radnog vremena, čime je prekršio interna pravila. Njegov poslodavac je nadgledao njegove komunikacije. Zapisi u kojima su vidljive poruke sasvim lične prirode objavljeni su u sklopu postupka

930 Radna grupa iz člana 29. (2017), *Mišljenje 2/2017 o obradi podataka na radnom mestu*, WP 249, Bruxelles, 8. juna 2017.

931 Radna grupa iz člana 29. (2005), Radni dokument o zajedničkom tumačenju člana 26. stav 1. Direktive 95/46/EZ od 24. oktobra 1995., WP 114, Bruxelles, 25. novembra 2005.

932 ESLJP, *Copland protiv Ujedinjenog Kraljevstva*, br. 62617/00, 3. aprila 2007.

933 ESLJP, *Bărbulescu protiv Rumunije* [VV], br. 61496/08, 5. septembra 2017, stav. 121.

u pred domaćim sudovima. ESLJP je utvrdio da je član 8. primenjiv u ovom slučaju,i ostavio otvorenim pitanje da li je na osnovu ograničavajućih pravila poslodavca podnosilac predstavke mogao razumno očekivati privatnost, ali zaključio je da poslodavac svojim uputstvima ne može sasvim da onemogući privatni društveni život na radnom mestu.

Kad je reč o osnovanosti takvog postupka, državama ugovornicama trebalo je omogućiti veliki raspon procena prilikom ocenjivanja potrebe za uspostavljanjem pravnog okvira kojim se regulišu uslovi u kojima poslodavac može da kontroliše elektronske i druge neposlovne komunikacije zaposlenih na radnom mestu. Uprkos tome, domaća tela morala su da obezbede da je poslodavčevo uvođenje mera za nadgledanje dopisivanja i drugih komunikacija, nezavisno od opsega i trajanja takvih mera, propraćeno odgovarajućim i dovoljnim zaštitnim merama protiv zloupotrebe. Srazmernost i procesne garancije protiv proizvoljnog postupanja bili su od ključne važnosti, a ESLJP je utvrdio niz činilaca koji su bili relevantni u tim okolnostima. Ti činioci su, između ostalog, uključivali meru u kojoj poslodavac nadgleda zaposlene, nivo mešanja u privatnost zaposlenih, posledice za zaposlene i postojanje odgovarajućih zaštitnih mera. Usto, domaća tela morala su da obezbede da zaposleni čije se komunikacije nadgledaju ima pristup pravnom leku pred pravosudnim telom sa nadležnošću da utvrdi, barem u suštini, kako se ti navedena merila poštuju i jesu li sporne mere zakonite.

U ovom slučaju ESLJP je utvrdio da je došlo do povrede člana 8., jer domaća tela nisu omogućila odgovarajuću zaštitu prava podnosioca predstavke na poštovanje njegovog privatnog života i prepiske, pa stoga nisu uspostavila pravičnu ravnotežu između predmetnih interesa.

Prema preporuci Saveta Evrope o zaposlenju, lične podatke koji se prikupljaju u svrhu zaposlenja treba dobiti direktno od zaposlenog pojedinca.

Lični podaci koji se prikupljaju radi zapošljavanja moraju se ograničiti na informacije koje su potrebne za procenu prikladnosti kandidata i njihovog radnog potencijala.

U Preporuci se takođe posebno spominju podaci o mišljenju o učinku ili mogućnostima pojedinih zaposlenih. Podaci o mišljenju moraju se zasnivati na pravičim i pravednim ocenama i ne smeju da budu formulisani na uvredljiv način. To je uslovljeno načelima pravične obrade podataka i tačnosti podataka.

Poseban vid zakonodavstva o zaštiti podataka u odnosu između zaposlenih i poslodavca je uloga predstavnika zaposlenih. Predstavnici smeju da primaju lične podatke

o zaposlenima samo ako je to nužno da bi mogli da zastupaju interese zaposlenih ili ako su takvi podaci nužni za ispunjavanje ili kontrolu obaveza utvrđenih kolektivnim ugovorima.

Osetljivi lični podaci koji se prikupljaju u svrhe rada smeju da se obrađuju samo u određenim slučajevima i u skladu sa zaštitnim merama koje se propisuju domaćim zakonodavstvom. Poslodavci mogu zaposlene ili kandidate za posao da pitaju o njihovom zdravstvenom stanju ili da ih podvrgnu zdravstvenom pregledu samo ako je to nužno. Razlozi za to mogu biti: utvrđivanje njihove prikladnosti za radno mesto, ispunjavanje zahteva preventivne medicine, zaštita vitalnih interesa ispitanika ili drugih zaposlenih i pojedinaca, omogućavanje dodele socijalnih davanja ili odgovaranje na sudske zahteve. Zdravstveni podaci smeju da se prikupljaju samo od dotičnog zaposlenog, a ne iz drugih izvora, osim uz izričit pristanak i pristanak utemeljen na informacijama ili ako je to propisano domaćim zakonodavstvom.

U skladu sa Preporukom o zaposlenju, zaposleni treba da budu informisani o svrsi obrade njihovih ličnih podataka, vrsti prikupljenih ličnih podataka, telima kojima se podaci redovno objavljuju kao i svrsi i pravnoj osnovi takvih objavljivanja. Elektronskim komunikacijama može se pristupiti na radnom mestu samo u svrhu bezbednosti ili drugih legitimnih razloga, a takav je pristup dozvoljen tek pošto zaposleni budu obavešteni da poslodavac može da pristupi takvim komunikacijama.

Zaposleni moraju imati pravo na pristup svojim podacima o zaposlenju, kao i pravo na njihovu ispravku ili brisanje. Ako se obrađuju podaci o mišljenju, zaposleni moraju imati pravo da ospore mišljenje. Međutim, ta prava mogu biti privremeno ograničena u svrhu unutrašnjih istraga. Ako se zaposlenom uskrati pristup, ispravka ili brisanje ličnih podataka o radu, domaćim zakonodavstvom moraju se propisati odgovarajući postupci kojima se osporava takvo uskraćivanje.

9.3. Zdravstveni podaci

Ključne tačke

- Medicinski podaci su osetljivi, zato uživaju posebnu zaštitu.

Lični podaci u vezi sa zdravljem ispitanika smatraju se posebnom kategorijom podataka u skladu sa članom 9. stav 1. Opšte uredbe o zaštiti podataka i članu 6. modernizovane Konvencije br. 108. Stoga, podaci u vezi sa zdravljem podležu stro-

žem režimu obrade podataka od neosetljivih podataka. Opštom uredbom o zaštiti podataka zabranjuje se obrada „ličnih podataka koji se odnose na zdravlje" (koji podrazumevaju „sve podatke koji se odnose na zdravstveno stanje ispitanika, a koji otkrivaju informacije u vezi s prethodnim, trenutnim ili budućim fizičkim ili mentalnim zdravstvenim stanjem ispitanika")[934], kao i genetičkih i biometrijskih podataka, osim ako je to dozvoljeno članom 9. stav 2. Obe te vrste podataka su dodate na popis „posebnih kategorija podataka"[935].

Primer: U predmetu *Z protiv Finske*[936] bivši suprug podnositeljke predstavke, koji je bio zaražen virusom HIV-a, učinio je niz polnih krivičnih dela. Kasnije je osuđen za ubistvo iz nehata, jer je svoje žrtve svesno izložio riziku od zaraze HIV-om. Domaći sud je naložio da celokupna presuda i dokumenti iz predmeta ostanu poverljivi 10 godina uprkos zahtevima podnositeljke predstavke za produženje perioda poverljivosti. Žalbeni sud je odbio te zahteve, a presuda je sadržala imena i prezimena i podnositeljke predstavke i njenog bivšeg supruga. ESLJP je smatrao da mešanje nije bilo nužno u demokratskom društvu, jer je zaštita medicinskih podataka od temeljne važnosti za ostvarenje prava na poštovanje privatnog i porodičnog života, naročito kad se radi o informacijama o zarazi HIV-om, jer je ta bolest stigmatizovana u mnogim društvima. Zato je ESLJP zaključio da je odobravanjem pristupa presudi žalbenog suda, u kojoj se navode identitet i zdravstveno stanje podnositeljke, po isteku perioda od 10 godina nakon donošenja presude, povređen član 8. EKLJP-a.

U okviru **prava EU**, članom 9 stav 2. tačka (h) Opšte uredbe o zaštiti podataka omogućava se obrada medicinskih podataka kada je ona nužna radi preventivne medicine, medicinske dijagnoze, pružanja zdravstvene zaštite ili tretmana ili u svrhu upravljanja zdravstvenim uslugama. Međutim, obrada je dozvoljena samo ako je vrši zdravstveni radnik koji ima obavezu čuvanja poslovne tajne ili drugo lice koje ima istu obavezu.

U okviru **prava Saveta Evrope**, u Preporuci Saveta Evrope o medicinskim podacima iz 1997. godine na obradu podataka u oblasti medicine detaljnije se primenjuju

934 Opšta uredba o zaštiti podataka, uvodna izjava 35.

935 *Ibid*., član 2.

936 ESLJP, *Z protiv Finske*, br. 22009/93, 25. februara 1997., st. 94 i 112.; videti i ESLJP, *M. S. protiv Švedske*, br. 20837/92, 27. avgusta 1997.; ESLJP, *L. L. protiv Francuske*, br. 7508/02, 10. oktobra 2006.; ESLJP, *I. Protiv Finske*, br. 20511/03, 17. jula 2008; ESLJP, *K. H. I drugi protiv Slovačke*, br. 32881/04, 28. aprila 2009; ESLJP, *Szuluk protiv Ujedinjenog Kraljevstva*, br. 36936/05, 2. juna 2009.

načela Konvencije br. 108[937]. Predložena su pravila u skladu s onima iz Opšte uredbe o zaštiti podataka u pogledu zakonitih svrha obrade medicinskih podataka, obaveza čuvanja poslovne tajne osoba koje upotrebljavaju zdravstvene podatke i prava ispitanika na transparentnost i pristup, ispravku i brisanje. Osim toga, medicinski podaci koje zdravstveni radnici zakonito obrađuju ne smeju se prenositi telima nadležnim za održavanje javnog reda i mira ako nisu obezbeđene „odgovarajuće zaštitne mere kojima se sprečava otkrivanje koje nije u skladu sa pravom na poštovanje [...] privatnog života koje je garantovano članom 8. Evropske konvencije o ljudskim pravima"[938]. Domaće zakonodavstvo, takođe, mora da bude „formulisano dovoljno precizno i obezbeđuje odgovarajuću pravnu zaštitu od proizvoljnosti"[939].

Osim toga, Preporuka o medicinskim podacima sadrži posebne odredbe o medicinskim podacima nerođene dece i nemoćnih osoba, kao i o obradi genetskih podataka. Naučna istraživanja izričito su priznata kao razlog za čuvanje podataka duže nego što su potrebni, iako to najčešće zahteva anonimizaciju. U članu 12. Preporuke o medicinskim podacima predlažu se detaljni propisi za situacije u kojima su istraživačima potrebni lični podaci, a anonimizirani podaci nisu dovoljni.

Pseudonimizacija može biti dobar način za ispunjavanje naučnih potreba i zaštitu interesa pacijenata. Koncept pseudonimizacije u kontekstu zaštite podataka detaljnije je objašnjen u delu 2.1.1.

Preporuka Saveta Evrope iz 2016. godine o podacima koji proizlaze iz genetičkih ispitivanja primenjuje se i na obradu podataka u oblasti medicine[940]. Preporuka je izuzetno važna za e-zdravstvo, u sklopu kojeg se informaciono-komunikacione tehnologije (IKT) upotrebljavaju za lakše pružanje zdravstvene zaštite. Primer je slanje rezultata testa očinstva nekog pacijenta od jednog pružaoca zdravstvenih usluga drugome. Cilj Preporuke je da se zaštite prava lica čiji se lični podaci obrađuju u svrhe obezbeđivanja protiv rizika u vezi sa zdravljem, telesnim integritetom, uzrastom ili smrću osobe. Osiguravajuća društva moraju da opravdaju obradu zdravstvenih podataka i ona mora biti proporcionalna prirodi i važnosti rizika koji se razmatra.

937 Savet Evrope, Komitet ministara (1997), Preporuka Rec(97)5 državama članicama o zaštiti medicinskih podataka, 13. februara 1997. Napominjemo da je u toku revizija te preporuke.

938 ESLJP, *Avilkina i drugi protiv Rusije*, br. 1585/09, 6. juna 2013, stav 53. Videti i ESLJP, *Biriuk protiv Litvanije*, br. 23373/03, 25 novembra 2008.

939 ESLJP, *L. H. protiv Latvije*, br. 52019/07, 29. aprila 2014., stav 59.

940 Savet Evrope, Komitet ministara (2016.), Preporuka Rec(2016)8 državama članicama o obradi ličnih zdravstvenih podataka u svrhu obezbeđenja, uključujući podatke iz genetičkih ispitivanja, 26. oktobra 2016.

Obrada ove vrste podataka zavisi od pristanka ispitanika. Osiguravajuća društva treba da uspostave i zaštitne mere za čuvanje zdravstvenih podataka.

Klinička ispitivanja, koja uključuju ocenjivanje efekata novih lekova na bolesnike u okruženjima dokumentovanih ispitivanja, imaju znatne implikacije na zaštitu podataka. Klinička ispitivanja lekova koji služe ljudskoj upotrebi regulisana se Uredbom (EU) br. 536/2014 Evropskog parlamenta i Saveta od 16. aprila 2014. o kliničkim ispitivanjima lekova za primenu kod ljudi i o stavljanju van snage Direktive 2001/20/EZ (Uredba o kliničkim ispitivanjima)[941]. Glavni elementi Uredbe o kliničkim ispitivanjima su:

- pojednostavljen postupak prijave putem portala EU[942],
- rokovi za ocenu zahteva za klinička ispitivanja[943],
- učestvovanje etičkog odbora u postupku ocenjivanja u skladu sa zakonima država članica (i evropskim pravom kojim se utvrđuju predmetni rokovi)[944] i
- poboljšana transparentnost kliničkih ispitivanja i njihovih ishoda[945].

U Opštoj uredbi o zaštiti podataka utvrđuje se da se u svrhe pristanka na učešće u aktivnostima naučnog istraživanja u sklopu kliničkih ispitivanja primenjuje Uredba (EU) br. 536/2014[946].

U toku su i mnoge druge zakonodavne i druge inicijative EU u vezi sa ličnim podacima u zdravstvenom sektoru[947].

941 Uredba (EU) br. 536/2014 Evropskog parlamenta i Saveta od 16. aprila 2014. o kliničkim ispitivanjima lekova za primenu kod ljudi i o stavljanju van snage Direktive 2001/20/EZ (Uredba o kliničkim ispitivanjima), SL 2014 L 158.

942 Uredba o kliničkim ispitivanjima, član 5. stav 1.

943 *Ibid*., član 5. stavovi od 2. do 5.

944 *Ibid*., član 2. stav 2. tačka 11.

945 *Ibid*., član 9. stav 1. i uvodna izjava 67.

946 Opšta uredba o zaštiti podataka, uvodne izjave 156 i 161.

947 EDPS (2013), Mišljenje Evropskog nadzornika za zaštitu podataka o izjavi Komisije o „Akcijskom planu za e-zdravlje 2012–2020: inovativno zdravstvo za 21. vek", Bruxelles, 27. marta 2013.

Elektronski zdravstveni kartoni

Elektronski zdravstveni kartoni definišu se kao „sveobuhvatan zdravstveni zapis ili slična dokumentacija o prošlom ili trenutnom telesnom i duševnom stanju pojedinca u elektronskom obliku, koji omogućavaju dostupnost tih podataka radi medicinskog lečenja i drugih usko povezanih svrha"[948]. Elektronski zdravstveni kartoni su elektronske verzije istorije bolesti bolesnika i mogu uključivati kliničke podatke koji se odnose na te pojedince, kao što su istorija bolesti, poteškoće i bolesti, lekovi i terapije, kao i rezultati pregleda i laboratorijski nalazi i izveštaji. Tim elektronskim datotekama, koje mogu da sadrže čitave kartone ili samo izvode ili sažetke, može pristupiti lekar opšte prakse, apotekar i drugi zdravstveni radnici. Koncept „e-zdravstva" takođe delimično dotiče ove zdravstvene kartone.

Primer: Osoba A ugovorila je polisu osiguranja s osiguravajućim društvom B. Društvo će prikupljati određene zdravstvene podatke od osobe A, kao što su trenutni zdravstveni problemi ili bolesti. Osiguravajuće društvo treba da čuva lične zdravstvene podatke osobe A odvojeno od drugih podataka. Osiguravajuće društvo treba da čuva i lične zdravstvene podatke odvojeno od drugih ličnih podataka. To znači da će samo osoba zadužena za predmet osobe A imati pristup njegovim zdravstvenim podacima.

Uprkos tome, elektronske zdravstvene datoteke dovode do određenih pitanja zaštite podataka, poput njihove dostupnosti, pravilnog čuvanja i pristupa ispitanika.

Uz elektronske zdravstvene kartone, 10. aprila 2014. godine Evropska komisija objavila je Zelenu knjigu o mobilnom zdravstvu („m-zdravstvu"), s obzirom na to da je m-zdravstvo nov, brzorastući sektor koji ima potencijal da transformiše zdravstvo i poveća njegovu delotvornost i kvalitet. Taj pojam obuhvata medicinsku i javnozdravstvenu praksu podržanu putem mobilnih uređaja kao što su mobilni telefoni, uređaji za praćenje bolesnika, lični digitalni pomoćnici i drugi bežični uređaji, kao i aplikacija (na primer, aplikacija za zdravlje) koje se mogu povezati sa medicinskim uređajima ili senzorima[949]. U Knjizi se navode rizici za pravo na zaštitu ličnih podataka koje razvoj m-zdravstva može doneti, pa se preporučuje da, s obzirom na ose-

948 Preporuka Komisije od 2. jula 2008. o prekograničnoj interoperabilnosti sistema elektronskih zdravstvenih kartona (dostupna na engleskom jeziku), tačka 3 (c).

949 Evropska komisija (2014), Zelena knjiga o mobilnom zdravstvu („m-zdravstvu"), COM(2014) 219 final, Bruxelles, 10. aprila 2014.

tljivu prirodu zdravstvenih podataka, njegov razvoj uključuje posebne i primerene bezbednosne i zaštitne mere za podatke bolesnika, kao što je šifrovanje, i odgovarajuće mehanizme provere autentičnosti bolesnika kako bi se umanjili bezbednosni rizici. Usklađenost sa propisima o zaštiti ličnih podataka, uključujući obavezu davanja informacija ispitaniku, bezbednost podataka i načelo zakonite obrade ličnih podataka, ključna je za izgradnju poverenja u rešenja m-zdravstva[950]. U tu svrhu stručnjaci su izradili Kodeks ponašanja na osnovu doprinosa širokog raspona učesnika, koji uključuju predstavnike sa stručnim iskustvom u zaštiti podataka, samostalnoj i zajedničkoj regulaciji, IKT-u i zdravstvu[951]. U vreme izrade ovog priručnika nacrt Kodeksa ponašanja podnesen je Radnoj grupi za zaštitu podataka iz člana 29. radi dodavanja napomena i njenog službenog odobrenja.

9.4. Obrada podataka u istraživačke i statističke svrhe

Ključne tačke

- Podaci koji se prikupljaju u statističke svrhe ili u svrhe naučnog ili istorijskog istraživanja ne smeju da se upotrebljavaju ni u koju drugu svrhu.
- Podaci koji se zakonito prikupljaju u bilo koju svrhu mogu se dalje upotrebljavati u statističke svrhe ili u svrhe naučnog ili istorijskog istraživanja pod uslovom da su uspostavljene odgovarajuće zaštitne mere. Anonimizacija ili pseudonimizacija pre prenosa podataka trećim osobama može pružiti te zaštitne mere.

Pravom EU omogućava se obrada podataka u statističke svrhe ili u svrhe naučnog ili istorijskog istraživanja pod uslovom da su uspostavljene odgovarajuće zaštitne mere za prava i slobode ispitanika. One mogu uključivati pseudonimizaciju[952]. Pravom EU ili pojedinih država mogu se odrediti određena odstupanja od prava ispitanika ako bi ta prava verovatno onemogućila ili ozbiljno ugrozila postizanje legitimne svrhe istraživanja[953]. Mogu se uvesti odstupanja od ispitanikovog prava na pristup, prava na ispravku, prava na ograničenje obrade i prava na prigovor.

950 *Ibid.*, str. 8.

951 Draft Code of Conduct on privacy for mobile health applications (Nacrt kodeksa ponašanja o privatnosti za mobilne aplikacije za zdravlje), 7. juna 2016.

952 Opšta uredba o zaštiti podataka, član 89. stav 1.

953 *Ibid.*, član 89. stav 2.

Iako podatke koje zakonito prikupi u bilo koju svrhu rukovalac podacima može ponovo iskoristiti u sopstvene statističke svrhe ili svrhe naučnog ili istorijskog istraživanja, podatke treba anonimizovati ili podvrgnuti postupcima kao što je pseudonimizacija, zavisno od konteksta, pre njihovog prenošenja trećoj osobi u statističke svrhe ili svrhe naučnog ili istorijskog istraživanja, osim ako je ispitanik za to dao svoj pristanak ili ako je to posebno propisano domaćim zakonodavstvom. Za razliku od anonimnih podataka, podaci podvrgnuti pseudonimizaciji i dalje podležu Opštoj uredbi o zaštiti podataka[954].

Uredbom se tako istraživanju dodeljuje poseban tretman u pogledu opštih propisa za zaštitu podataka kako bi se izbegla ograničenja razvoja istraživanja i postigla usklađenost sa ciljem uspostave evropskog istraživačkog prostora iz člana 179. UFEU. Njome se pruža široko tumačenje obrade ličnih podataka u svrhe naučnih istraživanja, uključujući tehnološki razvoj i demonstracije, osnovna istraživanja, primenjena istraživanja i istraživanja koja se finansiraju privatnim sredstvima. Takođe se prepoznaje važnost prikupljanja podataka u registrima u istraživačke svrhe i moguće poteškoće u tačnom utvrđivanju naknadne svrhe obrade ličnih podataka u svrhe naučnih istraživanja u trenutku prikupljanja podataka[955]. Zbog toga se Uredbom omogućava obrada podataka u te svrhe, bez pristanka ispitanika, pod uslovom da su uspostavljene odgovarajuće zaštitne mere.

Važan primer upotrebe podataka u statističke svrhe jesu službene statistike koje prikupe domaći zavodi za statistiku i zavodi za statistiku EU na osnovu domaćih zakonodavstava i zakonodavstva EU o zvaničnoj statistici. Prema tim propisima, građani i preduzeća uglavnom su dužni da otkriju podatke odgovarajućim telima nadležnima za statistiku. Službenici koji rade u zavodima za statistiku dužni su da čuvaju poslovnu tajnu. Tu svoju obavezu moraju propisno da ispunjavaju, jer je ona nužna da bi građani imali visok nivo poverenja i stavili svoje podatke na raspolaganje telima nadležnim za statistiku[956].

U Uredbi (EZ) br. 223/2009 o evropskoj statistici (Uredba o evropskoj statistici) sadržana su osnovna pravila zaštite podataka u kontekstu službene statistike koja se, stoga, mogu smatrati relevantnim i za odredbe o službenoj statistici na domaćem

954 *Ibid.*, uvodna izjava 26.

955 *Ibid.*, uvodne izjave 33, 157 i 159.

956 *Ibid.*, član 90.

nivou[957]. U Uredbi se zastupa načelo da je za službene statističke aktivnosti potrebna dovoljno jasna pravna osnova[958].

Primer: U predmetu *Huber protiv Bundesrepublik Deutschland*[959] austrijski preduzetnik koji se preselio u Nemačku požalio se da su nemačka tela prikupljanjem i čuvanjem ličnih podataka stranih državljana u centralnom registru (AZR), između ostalog u statističke svrhe, prekršile njegova prava na osnovu Direktive o zaštiti podataka. Budući da je Direktivom 95/46 nameravao da se obezbedi odgovarajući nivo zaštite podataka u svim državama članicama, SPEU je smatrao da se značenje koncepta nužnosti iz člana 7. tačka (e) ne može razlikovati među državama članicama, kako bi se obezbedio visok nivo zaštite u EU. Stoga je reč o konceptu koji ima sopstveno nezavisno značenje unutar prava EU i mora se tumačiti tako da u potpunosti odražava cilj Direktive 95/46. Napominjući da bi za statističke svrhe trebalo da budu potrebne samo anonimne informacije, SPEU je presudio da nemački registar nije u skladu sa zahtevom nužnosti iz člana 7. tačka (e).

U kontekstu **Saveta Evrope** dalja obrada podataka može se vršiti u naučne, istorijske ili statističke svrhe kada je to u javnom interesu i mora da podleže odgovarajućim zaštitnim merama[960]. Prava ispitanika mogu se ograničiti i prilikom obrade podataka u statističke svrhe, pod uslovom da ne postoji jasan rizik od kršenja njihovih prava i sloboda[961].

957 Uredba (EZ) br. 223/2009 Evropskog parlamenta i Saveta od 11. marta 2009. o evropskoj statistici i stavljanju van snage Uredbe (EZ, Euratom) br. 1101/2008 Evropskog parlamenta i Saveta o dostavi poverljivih statističkih podataka Statističkoj kancelariji Evropskih zajednica, Uredbe Saveta (EZ) br. 322/97 o statistici Zajednice i Odluke Saveta 89/382/EEZ, Euratom o osnivanju Odbora za statistički program Evropskih zajednica, SL 2009 L 87, kako je izmenjena Uredbom (EU) 2015/759 Evropskog parlamenta i Saveta od 29. aprila 2015. o izmeni Uredbe (EZ) br. 223/2009 o evropskoj statistici, SL 2015 L 123.

958 To načelo treba dodatno da se razradi u *Eurostatovom Kodeksu prakse* u kojem će se, u skladu s članom 11. Uredbe o evropskoj statistici, navoditi etičke smernice o načinu sprovođenja službene statistike, uključujući pažljivu upotrebu ličnih podataka.

959 SPEU, C-524/06, *Heinz Huber protiv Bundesrepublik Deutschland* [VV], 16. decembra 2008; vidi posebno sta 68.

960 Modernizovana Konvencija br. 108, član 5. stav 4. tačka (b).

961 *Ibid.*, član 11. stav 2.

Preporuka o statističkim podacima koja je izdana 1997. godine obuhvata vršenje statističkih aktivnosti u javnom i privatnom sektoru[962].

Podaci koje rukovalac podacima prikuplja u statističke svrhe ne smeju se upotrebljavati ni u koju drugu svrhu. Podaci prikupljeni u nestatističke svrhe moraju biti dostupni za dalju upotrebu u statističke svrhe. Preporukom o statističkim podacima omogućava se i prenošenje podataka trećim licima, pod uslovom da se to čini isključivo u statističke svrhe. U tim slučajevima bi strane trebalo da se dogovore i utvrde pisanim putem opseg zakonite dalje upotrebe u statističke svrhe. Budući da to ne zamenjuje pristanak ispitanika, po potrebi u domaćem zakonodavstvu moraju biti propisane odgovarajuće zaštitne mere radi smanjenja rizika od zloupotrebe ličnih podataka, kao što je obaveza anonimizacije ili pseudonimizacije podataka pre otkrivanja.

Stručnjaci za statistička istraživanja moraju biti obavezani posebnim dužnostima čuvanja poslovne tajne u sklopu domaćeg zakonodavstva, što je obično slučaj sa službenom statistikom. To se mora proširiti i na ispitivače i druge osobe koje prikupljaju lične podatke ako su zaposleni na prikupljanju podataka od ispitanika ili drugih osoba.

Ako upotreba ličnih podataka u statističkom istraživanju nije dopuštena zakonom, ispitanici možda treba da daju pristanak za upotrebu njihovih podataka ili barem da imaju mogućnost prigovora kako bi obrada bila legitimna. Ako ispitivači prikupljaju lične podatke u statističke svrhe, te osobe moraju biti jasno informisane o tome da li je davanje podataka obavezno prema domaćem zakonodavstvu.

Ako statističko istraživanje nije moguće vršiti s anonimizovanim podacima, već su nužni lični podaci, podaci prikupljeni u tu svrhu moraju se anonimizovati što pre. Na osnovu rezultata statističkog istraživanja u najmanju ruku ne sme biti moguće da se identifikuju ispitanici, osim ako to jasno ne predstavlja nikakav rizik.

Po završetku statističke analize lične podatke treba ili izbrisati ili anonimizovati. U tom slučaju se u Preporuci o statističkim podacima savetuje čuvanje identifikacionih podataka odvojeno od ostalih ličnih podataka. To na primer znači da se ključ za kodiranje ili popis sinonima za identifikaciju mora čuvati odvojeno od drugih podataka.

962 Savet Evrope, Komitet ministara (1997), Preporuka Rec(97)18 državama članicama o zaštiti ličnih podataka koji se prikupljaju i obrađuju u statističke svrhe, 30. septembra 1997.

9.5. Finansijski podaci

Ključne tačke

- Iako se finansijski podaci ne smatraju osetljivim podacima u smislu modernizovane Konvencije br. 108 ili Opšte uredbe o zaštiti podataka, za njihovu obradu su potrebne posebne zaštitne mere radi obezbeđenja tačnosti i sigurnosti podataka.
- Elektronski platni sistemi zahtevaju ugrađenu zaštitu podataka, odnosno privatnost ili tehničku i integrisanu zaštitu podataka.
- U toj oblasti dolazi do posebnih problema sa zaštitom podataka, jer treba primenjivati odgovarajuće mehanizme za autentifikaciju/potvrđivanje.

Primer: U predmetu *Michaud protiv Francuske*[963] podnosilac predstavke, francuski advokat, suprotstavio se svojoj obavezi prijave sumnji povezanih sa mogućim aktivnostima pranja novca koje vrše njegovi klijenti, na šta ga je obavezivalo francusko zakonodavstvo. ESLJP je istakao da je zahtevanje od advokata da upravnim telima prijavljuju informacije koje se odnose na drugu osobu, a koje su dobili putem službene komunikacije sa tom osobom, predstavlja mešanje u pravo advokata na poštovanje njihove prepiske i privatnog života prema članu 8. EKLJP-a, jer taj koncept obuhvata aktivnosti profesionalne ili poslovne prirode. Međutim, mešanje je bilo u skladu sa zakonom i imalo je legitimnu svrhu, tačnije sprečavanje nereda i zločina. Budući da advokati podležu obavezi prijavljivanja sumnjivih aktivnosti samo u vrlo ograničenim okolnostima, ESLJP je smatrao da je ta obaveza bila srazmerna. Zaključio je da nije došlo do povrede člana 8.

Primer: U predmetu *M. N. i drugi protiv San Marina*[964] podnosilac predstavke, građanin Italije, sklopio je fiducijarni ugovor sa kompanijom koja je bila pod istragom. To je značilo da je kompanija podvrgnuta pretresu i zapleni kopija (elektronske) dokumentacije. Podnosilac predstavke je podneo tužbu pred sudom u San Marinu, tvrdeći da ne postoji veza između njega i navodnih krivičnih dela. Međutim, sud je njegovu tužbu proglasio neprihvatljivom jer on

963 ESLJP, *Michaud protiv Francuske*, br. 12323/11, 6. decembra 2012. Videti i ESLJP, *Niemietz protiv Nemačke*, br. 13710/88, 16. decembra 1992, stav 29., i ESLJP, *Halford protiv Ujedinjenog Kraljevstva*, br. 20605/92, 25. juna 1997., stav 42.

964 ESLJP, *M. N. i drugi protiv San Marina*, br. 28005/12, 7. jula 2015.

nije bio „zainteresovana strana". ESLJP je smatrao da je ponosilac predstavke bio u veoma nepovoljnom položaju u pogledu sudske zaštite u odnosu na „zainteresovanu stranu", ali njegovi podaci su svejedno podlegali radnjama pretresa i zaplene. Stoga je ESLJP zaključio da je povređen član 8.

Primer: U predmetu *G. S. B. protiv Švajcarske*[965] pojedinosti o bankovnom računu podnosioca predstavke poslati su poreskoj upravi SAD na osnovu sporazuma o administrativnoj saradnji između Švajcarske i SAD. ESLJP je zaključio da se tim prenosom ne krši član 8. EKLJP-a jer je mešanje u pravo na privatnost podnosioca predstavke bilo propisano zakonom, imalo je legitiman cilj, tako da je bilo srazmerno javnom interesu o kojem je reč.

Primenu opšteg okvira za zaštitu podataka (kako je utvrđen u Konvenciji br. 108) na kontekst plaćanja razradio je **Savet Evrope** u Preporuci Rec(90)19 iz 1990. godine[966]. U toj preporuci je razjašnjen opseg zakonitog prikupljanja i upotrebe podataka u kontekstu plaćanja, naročito platnim karticama. U njoj se zakonodavcima predlažu detaljni propisi o pravilima u pogledu otkrivanja podataka o plaćanju trećim stranama, o vremenskim ograničenjima za zadržavanje podataka, o transparentnosti, bezbednosti podataka i prekograničnom prenosu podataka i, konačno, o nadzoru i pravnim lekovima. Savet Evrope izradio je Mišljenje o prenosu poreskih podataka[967], u kojem se navode preporuke i pitanja koje je potrebno uzeti u obzir prilikom prenosa poreskih podataka.

ESLJP dozvoljava prenos finansijskih podataka, tačnije pojedinosti o bankovnom računu pojedinca, na osnovu člana 8. EKLJP-a ako je to propisano zakonom, ima legitiman cilj i srazmerno je javnom interesu o kojem je reč[968].

Kad je reč o **pravu EU**, elektronski platni sistemi koji uključuju obradu ličnih podataka moraju da budu u skladu s Opštom uredbom o zaštiti podataka. Zato ti sistemi moraju pružati tehničku i integrisanu zaštitu podataka. Tehnička zaštita podataka podrazumeva da je rukovalac podacima dužan da uspostavi odgovarajuće tehničke i organizacione mere za sprovođenje načela zaštite podataka. Integrisana zaštita

965 ESLJP, *G. S. B. protiv Švajcarske*, br. 28601/11, 22. decembra 2015.

966 Savet Evrope, Komitet ministara (1990.), Preporuka br. R(90)19 o zaštiti ličnih podataka koji se upotrebljavaju za plaćanje i druge srodne radnje, 13. septembra 1990.

967 Savet Evrope, Savetodavni odbor Konvencije br. 108 (2014.), Mišljenje o uticaju mehanizama za automatsku međudržavnu razmenu podataka u upravne i poreske svrhe na zaštitu podataka, 4. juna 2014.

968 ESLJP, *G. S. B. protiv Švajcarske*, br. 28601/11, 22. decembra 2015.

podataka podrazumeva da rukovalac podacima mora obezbediti da se zadato obrađuju samo oni lični podaci koji su nužni u određenu svrhu (videti deo 4.4). U kontekstu finansijskih podataka, SPEU je smatrao da preneseni poreski podaci mogu predstavljati lične podatke[969]. Radna grupa iz člana 29. izdala je odgovarajuće smernice za države članice, koje su uključivale merila za obezbeđenje usklađenosti sa propisima o zaštiti podataka prilikom automatske razmene ličnih podataka u poreske svrhe putem automatizovanih sredstava[970].

Usto, donesen je niz pravnih instrumenata za uređenje finansijskih tržišta i aktivnosti kreditnih institucija i investicionih društava[971]. Ostali pravni instrumenti pomažu u suzbijanju trgovanja na osnovu povlašćenih informacija i manipulacija tržištem[972]. Najvažnije oblasti koje utiču na zaštitu podataka su:

- zadržavanje zapisa o finansijskim transakcijama,
- prenos ličnih podataka u treće zemlje,
- snimanje telefonskih razgovora ili elektronske komunikacije, uključujući ovlašćenje nadležnih tela da zatraže zapise o telefonskom saobraćaju i prometu podataka,
- otkrivanje ličnih informacija, uključujući objavu sankcija,
- ovlašćenje nadležnih tela da vrše nadzor i istrage, uključujući terenske preglede i ulazak u privatne prostorije radi oduzimanja dokumenata,
- mehanizmi za prijavu kršenja/povreda, npr. programi prijavljivanja nepravilnosti (uzbunjivači) i

969 SPEU, C-201/14, *Smaranda Bara i dr. protiv Casa Națională de Asigurări de Sănătate i dr.*, 1. oktobra 2015, stav 29.

970 Radna grupa za zaštitu podataka iz člana 29. (2015), Izjava Radne grupe za zaštitu podataka iz člana 29 o automatskim međudržavnim razmenama ličnih podataka u poreske svrhe, 14/EN WP 230.

971 Direktiva 2014/65/EU Evropskog parlamenta i Saveta od 15. maja 2014. o tržištu finansijskih instrumenata i izmeni Direktive 2002/92/EZ i Direktive 2011/61/EU, SL 2014 L 173; Uredba (EU) br. 600/2014 Evropskog parlamenta i Saveta od 15. maja 2014. o tržištima finansijskih instrumenata i izmeni Uredbe (EU) br. 648/2012, SL 2014 L 173; Direktiva 2013/36/EU Evropskog parlamenta i Saveta od 26. juna 2013. o pristupanju delatnosti kreditnih institucija i bonitetnom nadzoru nad kreditnim institucijama i investicionim kompanijama, izmeni Direktive 2002/87/EZ i stavljanju van snage direktiva 2006/48/EZ i 2006/49/EZ, SL 2013 L 176.

972 Uredba (EU) br. 596/2014 Evropskog parlamenta i Saveta od 16. aprila 2014. o zloupotrebi tržišta (Uredba o zloupotrebi tržišta) i stavljanju van snage Direktive 2003/6/EZ Evropskog parlamenta i Saveta i direktiva Komisije 2003/124/EZ, 2003/125/EZ i 2004/72/EZ, SL 2014 L 173.

- saradnja između nadležnih tela država članica i Evropskog nadzornog tela za vrednosne papire i tržišta kapitala (ESMA).

I druga pitanja su u tim oblastima posebno obrađena, uključujući prikupljanje podataka o finansijskom statusu ispitanika[973] ili prekograničnim plaćanjima putem bankovnih prenosa, što neizbežno dovodi do protoka ličnih podataka[974].

973 Uredba (EZ) br. 1060/2009 Evropskog parlamenta i Saveta od 16. septembra 2009. o agencijama za kreditni rejting, SL 2009 L 302, naknadno izmenjena Direktivom 2014/51/EU Evropskog parlamenta i Saveta od 16. aprila 2014. o izmeni direktiva 2003/71/EZ i 2009/138/EZ i uredbi (EZ) br. 1060/2009, (EU) br. 1094/2010 i (EU) br. 1095/2010 u pogledu ovlašćenja Evropskog nadzornog tela (Evropskog nadzornog tela za osiguranje i strukovno penziono osiguranje) i Evropskog nadzornog tela (Evropskog nadzornog tela za vrednosne papire i tržišta kapitala), SL 2014 L 153; Uredba (EU) br. 462/2013 Evropskog parlamenta i Saveta od 21. maja 2013. o izmeni Uredbe (EZ) br. 1060/2009 o agencijama za kreditni rejting, SL 2013 L 146.

974 Direktiva 2007/64/EZ Evropskog parlamenta i Saveta od 13. novembra 2007. o platnim uslugama na unutrašnjem tržištu i o izmeni direktiva 97/7/EZ, 2002/65/EZ, 2005/60/EZ i 2006/48/EZ i stavljanju van snage Direktive 97/5/EZ, SL 2007 L 319, kako je izmenjena Direktivom 2009/111/EZ Evropskog parlamenta i Saveta od 16. septembra 2009. o izmeni direktiva 2006/48/EZ, 2006/49/EZ i 2007/64/EZ u vezi sa bankama povezanim sa centralnim institucijama, određenim stavkama garantovanog kapitala, velikom izloženošću, nadzornim aranžmanima i upravljanjem u kriznim situacijama, SL 2009 L 302.

10

Savremeni izazovi u oblasti zaštite ličnih podataka

Digitalno doba, ili doba informacionih tehnologija, obeleženo je sveopštom upotrebom računara, interneta i digitalnih tehnologija. Ono uključuje prikupljanje i obradu velikih količina podataka, uključujući i lične podatke. Prikupljanje i obrada ličnih podataka u globalizovanoj ekonomiji podrazumevaju rast u oblasti prekograničnih prenosa podataka. Takva obrada nosi značajne i vidljive prednosti u svakodnevnom životu: internet pretraživači olakšavaju pristup velikim količinama informacija i znanja, društvene mreže omogućavaju ljudima širom sveta da komuniciraju, izražavaju svoja mišljenja i prikupljaju pomoć za društvene, ekološke i političke pokrete, a kompanije i potrošači ostvaruju korist od delotvornih marketinških metoda koje pokreću ekonomiju. Tehnologija i obrada ličnih podataka takođe su neizostavni alati za borbu domaćih tela protiv kriminala i terorizma. Isto tako, tzv. „veliki podaci", odnosno prikupljanje, čuvanje i analiza velikih količina informacija radi utvrđivanja uzoraka i predviđanja ponašanja, „mogu da budu izvor značajne vrednosti za društvo i povećaju produktivnost, učinak javnog sektora i društveno učestvovanje"[975].

Uprkos brojnim prednostima, digitalno doba donosi i određene izazove za privatnost i zaštitu podataka budući da se prikupljaju i obrađuju velike količine ličnih podataka na sve složenije i netransparentne načine. Tehnološki napredak doveo je do razvoja velikih grupa podataka koji mogu jednostavno unakrsno da se proveravaju i dalje

975 Savet Evrope, Savetodavni odbor Konvencije br. 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data* (Smernice o zaštiti pojedinaca u pogledu obrade ličnih podataka u svetu velikih podataka), T-PD(2017)01, Strasbourg, 23. januara 2017.

analiziraju kako bi se otkrili uzorci ili donosile odluke na osnovu algoritama, koji mogu dati sasvim nov uvid u ljudske navike i privatni život[976].

Nove tehnologije su moćne i mogu da budu posebno opasne ako dospeju u pogrešne ruke. Državna tela koja sprovode aktivnosti masovnog nadzora i upotrebljavaju te tehnologije primer su značajnog efekta koji te tehnologije mogu imati na prava pojedinaca. Informacije koje je Edvard Snouden otkrio 2013. godine o sprovođenju opsežnih programa nadzora interneta i telefona u obaveštajnim agencijama nekih američkih saveznih država izazvale su veliku zabrinutost o opasnostima koje aktivnosti nadzora nose za privatnost, demokratsko upravljanje i slobodu izražavanja. Masovni nadzor i tehnologije koje omogućavaju globalizovano čuvanje i obradu ličnih podataka i grupni pristup podacima mogli bi da naruše same temelje prava na privatnost[977]. Usto, mogli bi da imaju negativan efekat na političku kulturu i neželjene posledice po demokratiju, kreativnost i inovacije[978]. Već i sam strah da bi država mogla neprestano da prati i analizira ponašanje i postupke građana može ih odvratiti od izražavanja stavova o određenim pitanjima i dovesti do povećane opreznosti[979]. Ti izazovi su podstaknuli niz javnih tela, istraživačkih centara i organizacija civilnog društva da analiziraju moguće efekte novih tehnologija na društvo. Evropski nadzornik za zaštitu podataka pokrenuo je nekoliko inicijativa 2015. koje su bile usmerene na procenu efekta velikih podataka i interneta stvari (engl. *Internet of Things*) na etičnost. Između ostalog, osnovao je Savetodavnu grupu za etička pitanja koja za cilj ima podsticanje „otvorene i informisane rasprave o digitalnoj etici, što Evropskoj uniji omogućava uočavanje prednosti tehnologije za društvo i ekonomiju, uz istovremeno jačanje prava i slobode pojedinaca, naročito njihovog prava na privatnost i zaštitu podataka"[980].

976 Evropski parlament (2017.), *Rezolucija o uticaju velikih podataka na osnovna prava: privatnost, zaštita podataka, nediskriminacija, bezbednost i krivično gonjenje* (P8_TA-PROV(2017)0076), Strasbourg, 14. marta 2017.

977 Vidi UN, Generalna skupština, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism* (Izveštaj posebnog izvestioca o unapređenju i zaštiti ljudskih prava i osnovnih sloboda u borbi protiv terorizma), Ben Emmerson, A/69/397, 23. septembra 2014, st. 59. Videti i ESLJP, *Factsheet on Mass surveillance* (Informativni list o masovnom nadzoru), jul 2017.

978 EDPS (2015.), *Savladavanje izazova velikih podataka*, Mišljenje 7/2015, Bruxelles, 19. novembra 2015.

979 Vidi posebno SPEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr.* i *Kärntner Landesregierung i dr.* [VV], 8. aprila 2014, stav 37.

980 EDPS, Odluka od 3. decembra 2015. o uspostavi spoljašnje savetodavne grupe za etičke dimenzije zaštite podataka („Savetodavna grupa za etička pitanja"), 3. decembra 2015., uvodna izjava 5.

Obrada ličnih podataka je snažan alat i u rukama korporacija. Ona danas može da otkrije detaljne informacije o zdravlju ili finansijskoj situaciji osobe, koje zatim korporacije upotrebljavaju kako bi donosile važne odluke za pojedince, poput premija zdravstvenog osiguranja koje će se primenjivati na njih ili njihove kreditne sposobnosti. Metode obrade podataka mogu da utiču i na demokratske procese kada ih političari ili korporacije upotrebljavaju za uticanje na izbore, na primer „mikrociljanjem" poruka glasačima. Drugim rečima, iako se privatnost prvobitno smatrala pravom na zaštitu pojedinaca od neopravdanog mešanja tela javne vlasti, u novije doba ona može biti ugrožena i ovlašćenjima privatnih učesnika. Zbog toga se postavlja pitanje o upotrebi tehnologije i prediktivne analize u odlukama koje utiču na svakodnevni život pojedinaca, tako da se potvrđuje potreba da se obezbedi da se pri svakoj obradi ličnih podataka poštuju zahtevi osnovnih prava.

Zaštita podataka neraskidivo je povezana sa tehnološkim, društvenim i političkim promenama. Zato je nemoguće sastaviti celovit popis izazova koji bi mogli da se jave u budućnosti. U ovom poglavlju se razmatraju odabrane oblasti koje se odnose na velike podatke, internet društvene mreže i jedinstveno digitalno tržište EU. Nije reč o iscrpnoj proceni tih oblasti sa stanovišta zaštite podataka, nego se ističu brojni mogući međuodnosi novih ili izmenjenih ljudskih aktivnosti i zaštite podataka.

10.1. Veliki podaci, algoritmi i veštačka inteligencija

Ključne tačke

- Radikalne inovacije u području IKT-a oblikuju nov način života u sklopu kojeg su društveni odnosi, poslovanje, privatne i javne usluge međusobno digitalno povezani, što dovodi do stvaranja sve veće količine podataka, od kojih mnogi predstavljaju lične podatke.
- Vlade, preduzeća i građani sve više deluju u ekonomiji utemeljenoj na podacima, u kojoj su sami podaci postali vredna imovina.
- Koncept velikih podataka odnosi se na podatke i njihovu analitiku.
- Lični podaci koji se obrađuju u sklopu analitike velikih podataka potpadaju pod zakonodavstvo EU i Saveta Evrope.
- Odstupanja od propisa i prava na zaštitu podataka ograničena su na odabrana prava i određene situacije u kojima bi se sprovođenje prava pokazalo nemogućim ili bi zahtevalo nesrazmeran napor rukovaoca podacima.

- Potpuno automatizovano donošenje odluka po pravilu je zabranjeno, osim u određenim slučajevima.
- Svest među pojedincima i njihova kontrola ključni su za obezbeđenje sprovođenja prava.

U svetu koji je sve više digitalizovan, svaka aktivnost ostavlja digitalni trag koji se može prikupiti, obraditi i proceniti ili analizirati. Zahvaljujući novim informacionim i komunikacionim tehnologijama, sve se više podataka prikuplja i beleži[981]. Donedavno nijednom tehnologijom nije bilo moguće analizirati ili proceniti količinu podataka ili izvesti korisne zaključke. Podataka je jednostavno bilo previše da bi mogli da se procene, bili su previše složeni, loše strukturirani i prebrzo su se prenosili da bi se mogli utvrditi trendovi i navike.

10.1.1. Definisanje velikih podataka, algoritama i veštačke inteligencije

Veliki podaci

Pojam „velikih podataka" (engl. *big data*) jedan je od popularnih izraza današnjice koji može označavati nekoliko koncepata, u zavisnosti od konteksta. Obično obuhvata „sve veću tehnološku mogućnost prikupljanja, obrade i izdvajanja novih i prediktivnih saznanja iz velike količine, brzine i raznovrsnosti podataka"[982]. Koncept velikih podataka zato obuhvata i same podatke i analitiku podataka.

Podaci dolaze iz različitih vrsta **izvora**, koji uključuju osobe i njihove lične podatke, uređaje ili senzore, informacije o klimi, satelitske snimke, digitalne fotografije i video-zapise ili GPS signale. Međutim, veliki deo podataka i informacija čine lični podaci, odnosno ime, fotografija, adresa e-pošte, bankovni podaci, podaci za GPS

981 Evropska komisija, Komunikacija Komisije Evropskom parlamentu, Savetu, Evropskom ekonomskom i socijalnom odboru i Odboru regija, „Prema rastućoj ekonomiji utemeljenoj na podacima", COM(2014) 442 final, Bruxelles, 2. jula 2014.

982 Savet Evrope, Savetodavni odbor Konvencije br. 108, Smernice o zaštiti pojedinaca u pogledu obrade ličnih podataka u svetu velikih podataka, 23. januara 2017, str. 2.; Evropska komisija, Komunikacija Komisije Evropskom parlamentu, Savetu, Evropskom ekonomskom i socijalnom odboru i Odboru regija, „Prema rastućoj ekonomiji utemeljenoj na podacima", COM(2014) 442 final, Bruxelles, 2. jula 2014., str. 4.; Međunarodna telekomunikaciona unija (2015.), Preporuka Y.3600. Veliki podaci: zahtevi i mogućnosti utemeljeni na računarstvu u oblaku.

praćenje, objave na internet stranicama društvenih mreža, medicinski podaci ili IP adresa računara[983].

Pojam „veliki podaci" odnosi se i na **obradu**, analizu i procenu skupova podataka i dostupnih informacija, odnosno prikupljanje korisnih informacija u svrhu analize velikih podataka. To znači da se prikupljeni podaci i informacije mogu upotrebiti u svrhe koje se razlikuju od prvobitno predviđenih, na primer, za statističke trendove, ili za posebno prilagođene usluge kao što je oglašavanje. U slučajevima u kojima postoje tehnologije za prikupljanje, obradu i procenu velikih podataka, zapravo svaka vrsta informacija može da se kombinuje i ponovo proceni: finansijske transakcije, kreditna sposobnost, medicinsko lečenje, lična potrošnja, stručna delatnost, praćenje i odabrani putevi, upotreba interneta, elektronskih kartica i pametnih telefona, kao i video-nadzor ili nadzor komunikacija. Analizom velikih podataka dobija se nova kvantitativna dimenzija podataka koja se može proceniti i iskoristiti u stvarnom vremenu, na primer, radi pružanja prilagođenih usluga potrošačima.

Algoritmi i veštačka inteligencija

Veštačka inteligencija (VI) odnosi se na inteligenciju mašina koje deluju kao „inteligentni subjekti". Kao inteligentni subjekti, određeni uređaji uz pomoć softvera mogu da opažaju svoje okruženje i preduzimaju radnje na osnovu algoritama. Pojam VI primenjuje se kada uređaj oponaša „kognitivne" funkcije kao što su učenje i rešavanje problema, koje se obično povezuju sa ljudima[984]. Da bi oponašali donošenje odluka, moderne tehnologije i softveri upotrebljavaju algoritme koji omogućuju uređajima da donose „automatizovane odluke". Algoritam se najbolje može opisati kao postupni proces izračunavanja, obrade podataka, procene i automatizovanog rasuđivanja i donošenja odluka.

Slično kao i analitika velikih podataka, veštačka inteligencija i njeno automatizovano donošenje odluka zahtevaju kompilaciju i obradu velikih količina podataka. Ti podaci mogu proizlaziti iz samog uređaja (toplota kočnica, gorivo itd.) ili okruženja. Na primer, izrada profila je postupak koji se može zasnivati na automatizovanom donošenju odluka u skladu sa unapred određenim uzorcima ili faktorima.

983 Informativni list Komisije EU, „Reforma zaštite podataka u EU i veliki podaci", Savet Evrope, Savetodavni odbor Konvencije br. 108, Smernice o zaštiti pojedinaca u pogledu obrade ličnih podataka u svetu velikih podataka, 23. januara 2017, str. 2.

984 Stuart Russel i Peter Norvig, *Artificial Intelligence: A Modern Approach (2nd ed.)*, 2003, Upper Saddle River, New Jersey: Prentice Hall, str. 27, 32–58, 968–972; Stuart Russel i Peter Norvig, *Artificial Intelligence: A Modern Approach (3rd ed.)*, 2009, Upper Saddle River, New Jersey: Prentice Hall, str. 2.

Primer: Izrada profila i ciljano oglašavanje

Izrada profila na osnovu velikih podataka uključuje utvrđivanje uzoraka koji odražavaju „obeležja određenog tipa ličnosti", na primer kada kompanije za internet prodaju predlažu proizvode uz izraz „moglo bi da vam se svidi" na osnovu informacija prikupljenih od proizvoda koje je korisnik prethodno stavio u korpu za kupovinu. Što je više podataka dostupno, to je slika jasnija. Na primer, pametni telefoni su važan upitnik koji pojedinci ispunjavaju pri svakoj upotrebi, bilo svesno bilo nesvesno.

Savremena psihografija, nauka koja proučava ličnosti, zasniva se na metodi OCEAN prema kojoj određuje pojedini tip ličnosti. Pet osnovnih dimenzija ličnosti (engl. *Big Five*) odnosi se na otvorenost prema iskustvima (Openness) (koliko je osoba otvorena prema novostima), savesnost (Conscientiousness) (koliko je osoba sklona perfekcionizmu), ekstravertnost (Extraversion) (koliko je osoba društvena), prijatnost (Agreeableness) (koliko je osoba prijatna) i neurotičnost (Neuroticism) (koliko je osoba osetljiva). Na osnovu tih informacija moguće je izraditi profil dotične osobe, njenih potreba i strahova, ponašanja itd. Profil se zatim dopunjuje drugim informacijama o osobi koje se dobijaju iz svih dostupnih izvora, od posrednika za podatke, sa društvenih mreža (uključujući oznake „Sviđa mi se" za objave i objavljene fotografije), iz muzike koja se sluša putem interneta ili GPS podataka ili podataka o praćenju.

Grupe profila koji se izrađuju na osnovu metoda analize velikih podataka tada se upoređuju kako bi se utvrdili slični uzorci i oblikovale grupe ličnosti. Stoga se informacije o ponašanju i stavovima određenih ličnosti preokreću. Zahvaljujući pristupu velikim podacima i njihovoj upotrebi, preokreće se test ličnosti pa se informacije o ponašanju i stavovima sada koriste za opis ličnosti pojedinca. Kombinovanjem informacija o oznakama „Sviđa mi se" na društvenim mrežama, podataka o praćenju, muzike koja se sluša ili pogledanih filmova, dobija se jasna slika ličnosti pojedinca, što kompanijama omogućava da prenose prilagođene oglase i/ili informacije u skladu sa tipom „ličnosti" te osobe. Povrh svega, te informacije mogu da se obrađuju u stvarnom vremenu[985].

985 Metodama obrade i novim softverom u stvarnom vremenu se procenjuju informacije o tome šta se nekoj osobi sviđa, šta gleda prilikom kupovine putem interneta ili šta dodaje u korpu za kupovinu tako da bi se mogli predlagati „proizvodi" koji bi joj se mogli svideti na osnovu prikupljenih informacija.

10.1.2. Procena koristi i rizika velikih podataka

Savremene metode obrade mogu da podnesu velike količine podataka, brzo uvođenje novih podatka, pruže obradu informacija u stvarnom vremenu zahvaljujući kratkom vremenu odziva (čak i u slučaju složenih zahteva), omoguće višestruke i istovremene zahteve i analiziraju različite vrste informacija (fotografije, tekstove ili brojeve). Te tehnološke inovacije omogućuju strukturiranje, obradu i procenu skupova podataka i informacija u stvarnom vremenu[986]. Eksponencijalnim povećanjem količine podataka koji su dostupni i koji se analiziraju mogu se postići rezultati koji bi bili nemogući u slučaju analize manjeg opsega. Veliki podaci pomogli su u razvoju nove oblasti poslovanja u sklopu koje mogu početi da se pružaju nove usluge i preduzećima i pojedincima. Vrednost ličnih podataka građana EU mogla bi da naraste na gotovo 1 trilion EUR godišnje do 2020[987]. Zato veliki podaci mogu da pruže nove **mogućnosti** koje proizlaze iz procene grupnih podataka za nove društvene, ekonomske ili naučne uvide koji mogu da koriste pojedincima, preduzećima i vladama[988].

Analitika velikih podataka može otkriti uzorke među različitim izvorima i grupama podataka, koji mogu pružiti korisne uvide u oblasti poput nauke i medicine. Na primer, to je slučaj s oblastima kao što su zdravstvo, bezbednost hrane, inteligentni sistemi prevoza, energetska efikasnost ili urbanističko planiranje. Takva analiza informacija u stvarnom vremenu može se upotrebiti za poboljšanje uvedenih sistema. U istraživanjima se novi uvidi mogu ostvariti kombinovanjem velike količine podataka i statističkih procena, naročito u disciplinama u kojima su se do sada podaci uveliko ručno procenjivali. Mogu se razviti nove terapije prilagođene pojedinim pacijentima na osnovu poređenja sa grupom dostupnih informacija. Kompanije se nadaju da

986 Razvoj softvera za obradu velikih količina podataka još je u začecima. Međutim, nedavno su razvijeni analitički programi, naročito za analizu grupnih podataka i informacija u stvarnom vremenu povezanih s aktivnostima pojedinaca. Mogućnost analiziranja i obrađivanja velike količine podataka na strukturiran način omogućila je novi oblik izrade profila i ciljanog oglašavanja. Evropska komisija, Komunikacija Komisije Evropskom parlamentu, Savetu, Evropskom ekonomskom i socijalnom odboru i Odboru regija, „Prema rastućoj ekonomiji zasnovanoj na podacima", COM(2014) 442 final, Bruxelles, 2. jula 2014. ; Informativni list Komisije EU-a, „Reforma zaštite podataka u EU-u i veliki podaci" i Savet Evrope, „Smernice o zaštiti pojedinaca u pogledu obrade ličnih podataka u svetu velikih podataka", 23. januara 2017., str. 2.

987 Informativni list Komisije EU-a, „Reforma zaštite podataka u EU i veliki podaci".

988 Međunarodna konferencija poverenika za zaštitu podataka i privatnost (2014), Rezolucija o velikim podacima i Evropska komisija, Komunikacija Komisije Evropskom parlamentu, Savetu, Evropskom ekonomskom i socijalnom odboru i Odboru regija, „Prema rastućoj ekonomiji zasnovanoj na podacima", COM(2014) 442 final, Bruxelles, 2. jula 2014., str. 2.; Informativni list Komisije EU-a, „Reforma zaštite podataka u EU i veliki podaci" te Savet Evrope, Smernice o zaštiti pojedinaca u pogledu obrade ličnih podataka u svetu velikih podataka, 23. januara 2017., str. 1.

će im analiza velikih podataka omogućiti ostvarenje konkurentne prednosti, doneti moguće uštede i stvoriti nove oblasti poslovanja putem neposredne, individualizovane usluge usmerene na korisnike. Državne agencije nadaju se da će ostvariti poboljšanja u krivičnom pravosuđu. U Strategiji jedinstvenog digitalnog tržišta za Evropu Evropske komisije prepoznat je potencijal tehnologija i usluga koje pokreću podaci i velikih podataka da deluju kao pokretači ekonomskog rasta, inovacija i digitalizacije u EU[989]. Međutim, veliki podaci nose i određene **rizike** koji se obično povezuju sa količinom, brzinom i raznolikošću obrađenih podataka. Reč je zapravo o količini obrađenih podataka, broju i raznovrsnosti podataka, odnosno brzini obrade podataka. Posebna pitanja zaštite podataka javljaju se kada se analitika velikih podataka upotrebljava na velikim skupovima podataka radi izdvajanja novih i prediktivnih saznanja u svrhe donošenja odluka o pojedincima i/ili grupama[990]. Rizici za zaštitu podataka i privatnost povezani sa velikim podacima istaknuti su u mišljenjima Radne grupe iz člana 29., rezolucijama Evropskog parlamenta i dokumentima sa politikama Saveta Evrope[991].

Rizici mogu uključivati pogrešno postupanje sa velikim podacima onih koji imaju pristup grupnim informacijama putem manipulacije, diskriminacije ili ugnjetavanja pojedinaca ili pojedinih grupa u društvu[992]. Kada se grupe ličnih podataka ili informacija o ponašanju pojedinaca prikupljanju, obrađuju i procenjuju, njihovo iskorišćavanje može dovesti do značajnih povreda osnovnih prava i sloboda izvan prava na privatnost. Merenje tačne razmere u kojoj to može uticati na privatnost i lične podatke nije moguće. Evropski parlament utvrdio je da nedostaje metodologija za procenu celokupnog učinka velikih podataka na osnovu dokaza, ali postoje dokazi koji ukazuju na to da analitika velikih podataka može imati značajan horizontalni uticaj na javni i privatni sektor[993].

989 Rezolucija Evropskog parlamenta od 14. marta 2017. o uticaju velikih podataka na osnovna prava: privatnost, zaštita podataka, nediskriminacija, bezbednost i krivično gonjenje (2016/2225 (INI)).

990 Savet Evrope, Savetodavni odbor Konvencije br. 108, Smernice o zaštiti pojedinaca u pogledu obrade ličnih podataka u svetu velikih podataka, 23. januara 2017., str. 2.

991 Na primer, vidi EDPS (2015.), *Savladavanje izazova velikih podataka*, Mišljenje 7/2015, 19. novembra 2015.; EDPS (2016.), *Dosledno jačanje osnovnih prava u doba velikih podataka*, Mišljenje 8/2016, 23. septembra 2016.; Evropski parlament (2016.), Rezolucija o uticaju velikih podataka na osnovna prava: privatnost, zaštita podataka, nediskriminacija, bezbednost i krivično gonjenje (P8_TA(2017)0076), Strasbourg, 14. marta 2017.; Savet Evrope, Savetodavni odbor Konvencije br. 108, Smernice o zaštiti pojedinaca u pogledu obrade ličnih podataka u svetu velikih podataka, T-PD(2017)01, Strasbourg, 23. januara 2017.

992 Međunarodna konferencija poverenika za zaštitu podataka i privatnost (2014.), Rezolucija o velikim podacima.

993 Rezolucija Evropskog parlamenta od 14. marta 2017. o uticaju velikih podataka na osnovna prava: privatnost, zaštita podataka, nediskriminacija, bezbednost i krivično gonjenje (2016/2225 (INI)).

Opšta uredba o zaštiti podataka sadrži odredbe o pravu da se na pojedinca ne odnosi odluka koja se zasniva na automatizovanoj obradi, uključujući izradu profila[994]. Pitanje privatnosti javlja se kada ostvarivanje prava na prigovor zahteva ljudsku intervenciju, kojom se ispitanicima omogućava da izraze svoj stav i ospore odluku[995]. Iz toga mogu proizaći izazovi u pogledu obezbeđenja odgovarajućeg nivoa zaštite ličnih podataka ako, na primer, ljudska intervencija nije moguća ili ako su algoritmi previše složeni, a količina podataka prevelika da bi se pojedincima pružila obrazloženja za određene odluke i/ili da bi im se dale prethodne informacije kako bi se dobio njihov pristanak. Primer upotrebe veštačke inteligencije i automatizovanog donošenja odluka vidljiv je u novim pojavama u oblasti zahteva za hipoteke ili tokom procesa zapošljavanja. Zahtevi i prijave odbijaju se ili odbacuju na osnovu činjenice da podnosioci ne ispunjavaju predodređene parametre ili faktore.

10.1.3. Problemi u vezi sa zaštitom podataka

U kontekstu zaštite podataka, osnovni problemi, sa jedne se strane, odnose na količinu i raznolikost ličnih podataka koji se obrađuju, a sa druge na obradu i njene rezultate. Uvođenje složenih algoritama i softvera za pretvaranje grupnih podataka u izvor za donošenje odluka posebno utiče na pojedince i grupe, najviše u slučaju izrade profila ili označavanja, i na kraju dovodi do brojnih problema u vezi sa zaštitom podataka[996].

Utvrđivanje rukovaoca podacima i obrađivača podataka i njihove odgovornosti

Veliki podaci i veštačka inteligencija dovode do niza pitanja u vezi s utvrđivanjem rukovaoca podacima i obrađivača podataka i njihovom odgovornošću: kada se prikuplja i obrađuje toliko velika količina podataka, ko je vlasnik podataka? Kada podatke obrađuju inteligentne mašine i softver, ko je rukovalac podacima? Koje su tačne odgovornosti svakog učesnika obrade? U koje svrhe se mogu upotrebljavati veliki podaci?

Problem odgovornosti u kontekstu VI dodatno će se otežati kada VI donese odluku utemeljenu na obradi podataka koju sam razvije. Opšta uredba o zaštiti podataka pruža pravni okvir za odgovornost rukovaoca podacima i obrađivača podataka.

994 Opšta uredba o zaštiti podataka, član 22.

995 *Ibid.*, član 22. stav 3.

996 Savet Evrope, Savetodavni odbor Konvencije br. 108, Smernice o zaštiti pojedinaca u pogledu obrade ličnih podataka u svetu velikih podataka, 23. januara 2017, str. 2.

Nezakonitom obradom ličnih podataka nastaje odgovornost za rukovaoca podacima i obrađivača podataka[997]. Pri upotrebi veštačke inteligencije i automatizovanog donošenja odluka postavlja se pitanje o tome ko snosi odgovornost za povrede privatnosti ispitanika kada se složenost i količina obrađenih podataka ne mogu tačno utvrditi. U slučajevima u kojima se veštačka inteligencija i algoritmi smatraju proizvodima, javlja se problem lične odgovornosti, koja je uređena Opštom uredbom o zaštiti podataka, i odgovornosti za proizvod, koja nije uređena Uredbom[998]. Za to su potrebni propisi o odgovornosti kako bi se ispunila praznina između lične odgovornosti i odgovornosti za proizvod, na primer za robotiku i VI, uključujući automatizovano donošenje odluka[999].

Uticaj na načela zaštite podataka

Priroda, analiza i upotreba gore opisanih velikih podataka dovode u pitanje primenu određenih tradicionalnih, temeljnih načela evropskog prava zaštite podataka[1000]. Izazovi se uglavnom odnose na načela zakonitosti, smanjenja količine podataka, ograničenja svrhe i transparentnosti.

U skladu sa načelom smanjenja količine podataka, lični podaci moraju biti prikladni, relevantni i ograničeni na ono što je nužno u svrhe u koje se obrađuju. Međutim, poslovni model velikih podataka mogao bi biti sušta suprotnost smanjenju količine podataka budući da zahteva sve više i više podataka, često u neodređene svrhe.

To se odnosi i na načelo ograničenja svrhe, prema kojem podaci moraju da se obrađuju u određene svrhe i ne smeju da se upotrebljavaju u svrhe koje nisu u skladu sa prvobitnom svrhom prikupljanja, osim ako se takva obrada zasniva na nekoj pravnoj osnovi, kao što je, između ostalog, pristanak ispitanika (videti deo 4.1.1).

997 Opšta uredba o zaštiti podataka, članovi od 77. do 79. i član 82.

998 Evropski parlament, evropska Pravila građanskog prava o robotici, Opšta uprava za unutarnju politiku, (oktobar 2016), str. 14.

999 Govor Roberta Viole (dostupan na engleskom jeziku) na medijskom seminaru o evropskim zakonima o robotici u Evropskom parlamentu. (SPEECH 16/02/2017); objava Evropskog parlamenta (dostupna na engleskom jeziku) o zahtevu Komisiji za predlog Pravila o građanskopravnoj odgovornosti za robotiku i veštačku inteligenciju.

1000 Savet Evrope, Smernice o zaštiti pojedinaca u pogledu obrade ličnih podataka u svetu velikih podataka, T-PD (2017) 01, Strasbourg, 23. januara 2017.

Konačno, veliki podaci dovode u pitanje i načelo tačnosti podataka, budući da se u takvim primenama najčešće prikupljaju podaci iz različitih izvora bez mogućnosti provere i/ili obezbeđenja tačnosti prikupljenih podataka[1001].

Posebna pravila i prava

Opšte pravilo je da lični podaci koji se obrađuju u sklopu analitike velikih podataka potpadaju pod oblast primene zakonodavstva o zaštiti podataka. Uprkos tome, u pravu EU i Saveta Evrope uvedena su posebna pravila ili odstupanja u određenim slučajevima koji se odnose na složenu algoritamsku obradu podataka.

U sklopu prava Saveta Evrope, modernizovanom Konvencijom br. 108 ispitanicima se dodeljuju nova prava kako bi se obezbedio njihov delotvorniji nadzor nad sopstvenim ličnim podacima u doba velikih podataka. Na primer, to je slučaj sa članom 9. stav 1. tačke (a), (c) i (d) modernizovane Konvencije, koje se odnose na pravo da se na lice ne primenjuje odluka koja značajno utiče na nju, a koja se zasniva na automatizovanoj obradi podataka, bez uzimanja u obzir stava te osobe; na pravo da se na zahtev dobiju informacije o razlozima za obradu podataka ako se rezultati takve obrade odnose na nju i pravo na prigovor. Ostale odredbe modernizovane Konvencije br. 108, najviše odredbe o transparentnosti i dodatnim obavezama, dopunjavaju zaštitni mehanizam uspostavljen modernizovanom Konvencijom br. 108 za suočavanje s izazovima digitalnih tehnologija.

Osim u slučajevima iz člana 23. OUZP-a, pravom Unije mora se obezbediti **transparentnost** svake obrade ličnih podataka. Ona je posebno važna u pogledu internet usluga i drugih složenih oblika automatizovane obrade podataka, poput upotrebe algoritama za donošenje odluka. U tom kontekstu, svojstva sistema za obradu podataka moraju ispitanicima omogućiti da zaista razumeju šta se dešava sa njihovim podacima. Da bi se obezbedila poštena i transparentna obrada, Opštom uredbom o zaštiti podataka od rukovodioca podacima zahteva se da ispitaniku pruži smislene informacije o logici automatizovanog donošenja odluka, uključujući izradu profila[1002].U Preporuci o zaštiti i unapređenju prava na slobodu izražavanja i prava na privatni život u pogledu mrežne neutralnosti, Komitet ministara Saveta Evrope preporučio je da pružaoci internet usluga „pružaju korisnicima jasne, potpune i javno dostupne informacije o svim praksama upravljanja prometom koje bi mogle da utiču

1001 EDPS (2016), Dosledno jačanje osnovnih prava u doba velikih podataka, Mišljenje 8/2016, 23. septembra 2016, str. 8.

1002 Opšta uredba o zaštiti podataka, član 13. stav 2. tačka (f).

na pristup korisnika sadržaju, aplikacijama ili uslugama ili njihovu distribuciju"[1003]. Izveštaji o praksama upravljanja potrošnje interneta, koje sastavljaju nadležna tela u svim državama članicama, treba da se pripreme na otvoren i transparentan način i besplatno stave na raspolaganje javnosti[1004].

Rukovaoci podacima moraju da **obaveste** ispitanike **–** i kada su podaci prikupljeni od njih i kada nisu – ne samo o tačnim informacijama o prikupljenim podacima i predviđenoj obradi (videti deo 6.1.1), nego po potrebi i o postojanju automatizovanih postupaka donošenja odluka, uključujući „smislene informacije o tome o kojoj je logici reč"[1005], ciljeve i moguće posledice takvih procesa. U Opštoj uredbi o zaštiti podataka objašnjava se i (samo u slučajevima u kojima lični podaci nisu dobijeni od ispitanika) da rukovalac podacima nije dužan da dâ ispitaniku takve informacije ako je „davanje takvih informacija nemoguće […] ili bi zahtevalo nesrazmerne napore"[1006]. Međutim, kako ističe Radna grupa iz člana 29. u *Smernicama o automatizovanom pojedinačnom donošenju odluka i izradi profila za potrebe Uredbe 2016/679,* složenost obrade sama po sebi ne bi smela da spreči rukovaoca podacima da ispitaniku da jasna obrazloženja ciljeva i analitike koja je upotrebljena za obradu podataka[1007].

Prava ispitanika na **pristup** sopstvenim ličnim podacima i njihovu **ispravku** i **brisanje**, kao i pravo na **ograničenje** obrade ne sadrže slično izuzeće. Međutim, obaveza rukovaoca podacima da obavesti ispitanika o svakoj ispravci ili brisanju njegovih ličnih podataka (vidi deo 6.1.4) može da se ukine ako se takvo obaveštavanje „pokaže nemogućim ili zahteva nesrazmeran napor"[1008].

Ispitanici takođe imaju pravo na **prigovor** u skladu sa članom 21. OUZP-a (vidi deo 6.1.6) na svaku obradu svojih ličnih podataka, između ostalog i u slučaju analitike velikih podataka. Iako se rukovaoci podacima mogu izuzeti iz te obaveze ako mogu da dokažu prevladavajuće legitimne interese, nemaju pravo na takvo izuzeće u slučaju obrade u svrhe direktnog marketinga.

1003 Savet Evrope, Komitet ministara (2016), Preporuka CM/Rec(2016)1 Odbora ministara državama članicama o zaštiti i unapređenju prava na slobodu izražavanja i prava na privatni život u pogledu mrežne neutralnosti, 13. januara 2016, stav 5.1.

1004 *Ibid.*, stav 5.2.

1005 Opšta uredba o zaštiti podataka, član 13. stav 2. tačka (f) i član 14. stav 2. tačka (g).

1006 *Ibid.*, član 14. stav 5. tačka (b).

1007 Radna grupa iz člana 29., *Smernice o automatiziranom pojedinačnom donošenju odluka i izradi profila za potrebe Uredbe 2016/679*, WP 251, 3. oktobra 2017., str. 14.

1008 Opšta uredba o zaštiti podataka, član 19.

Rukovalac podacima može da zatraži posebna odstupanja od tih prava i u slučaju obrade ličnih podataka za potrebe arhiviranja u javnom interesu, u svrhe naučnog ili istorijskog istraživanja ili u statističke svrhe[1009].

U pogledu **izrade profila i automatizovanog donošenja odluka** OUZP-om su uvedena posebna pravila: U članu 22. stav 1. utvrđuje se da ispitanik „ima pravo da se na njega ne odnosi odluka koja se zasniva isključivo na automatizovanoj obradi, koja proizvodi pravne efekte koji se na njega odnose". Kako se ističe u smernicama Radne grupe iz člana 29., ovim članom se utvrđuje opšta zabrana potpuno automatizovanog donošenja odluka[1010]. Rukovaoci podacima mogu da budu izuzeti iz takve zabrane samo u tri posebna slučaja, odnosno ako je odluka: 1) potrebna za zaključenje ili izvršenje ugovora između ispitanika i rukovaoca podacima, 2) dozvoljena pravom Unije ili države članice ili 3) utemeljena na izričitom pristanku ispitanika[1011].

Lična kontrola

Složenost i nedostatak transparentnosti analitike velikih podataka mogli bi da zahtevaju promene u shvatanju lične kontrole nad ličnim podacima. Ona bi trebalo da bude prilagođena datom društvenom i tehnološkom kontekstu, uzimajući u obzir nedostatak informacija pojedinaca. Zato bi u zaštiti podataka u vezi sa velikim podacima trebalo da se usvoji širi koncept kontrole nad upotrebom podataka, prema kojem se lična kontrola razvija u složeniji postupak višestrukih procena efekata rizika povezanih s upotrebom podataka[1012].

Koliko je neka aplikacija velikih podataka dobra zavisi od toga koliko precizno može da predvidi želje i ponašanje pojedinaca (ili potrošača) koji je testiraju. Postojeći prognostički modeli koji se temelje na analitici velikih podataka neprekidno se usavršavaju. Inovacije uključuju ne samo upotrebu podataka za kategorizaciju tipova ličnosti (odnosno ponašanja i stavova), nego i analizu ponašanja putem analize glasovnih obrazaca i intenziteta pisanja poruka ili telesne temperature. Sve te informacije se mogu upotrebljavati u stvarnom vremenu u odnosu na saznanja koja proizlaze iz procena velikih podataka, na primer za procenu kreditne sposobnosti tokom sastanka sa bankarom. Procena se ne donosi na osnovu zasluga osobe koja

1009 *Ibid.*, član 89. stavovi 2. i 3.

1010 Radna grupa iz člana 29., *Smernice o automatiziranom pojedinačnom donošenju odluka i izradi profila za potrebe Uredbe 2016/679*, WP 251, 3. oktobra 2017., str. 9.

1011 Opšta uredba o zaštiti podataka, član 22. stav 2.

1012 Savet Evrope, Savetodavni odbor Konvencije br. 108, Smernice o zaštiti pojedinaca u pogledu obrade ličnih podataka u svetu velikih podataka, T-PD(2017)01, Strasbourg, 23. januara 2017.

podnosi zahtev za kredit, nego na obeležjima ponašanja koja proizlaze iz analize i procene velikih podataka, odnosno govora snažnim ili prijatnim glasom, govora tela ili telesne temperature.

Izrada profila i ciljano oglašavanje ne moraju nužno da budu problematični ako su osobe **svesne** da su podvrgnute posebno prilagođenim oglasima. Izrada profila postaje problem kada se upotrebljava za manipulisanje pojedincima, npr. za traženje određenih tipova ličnosti ili grupa lica za političke kampanje. Na primer, grupama neodlučnih glasača mogu biti upućene političke poruke prilagođene njihovoj ličnosti i stavovima. Drugi mogući problem je upotreba izrade profila za uskraćivanje pristupa određenih pojedinaca proizvodima i uslugama. Jedna zaštitna mera kojom se može obezbediti zaštita od zloupotrebe velikih podataka i ličnih podataka jeste pseudonimizacija (videti deo 2.1.1)[1013]. Kada su lični podaci potpuno anonimizovani, odnosno ne sadrže informacije koje se mogu povezati s ispitanikom, ti slučajevi izlaze iz područja primene Opšte uredbe o zaštiti podataka. Pristanak ispitanika i pojedinaca u kontekstu obrade velikih podataka takođe predstavlja izazov za zakonodavstvo o zaštiti podataka. To obuhvata pristanak na dobijanje prilagođenih oglasa i izradu profila, koji se mogu opravdati razlozima „korisničkog iskustva", i pristanak na upotrebu grupa ličnih podataka za usavršavanje i razvoj analitičkih alata koji se zasnivaju na informacijama. Svest o obradi velikih podataka, ili nedostatak iste, dovodi do nekoliko pitanja u vezi sa sredstvima putem kojih ispitanici mogu da ostvare svoja prava, s obzirom na to da se obrada velikih podataka može zasnivati i na pseudonimizovanim i anonimizovanim podacima koji su podvrgnuti algoritmima. Dok su pseudonimizovani podaci obuhvaćeni Opštom uredbom o zaštiti podataka, Uredba se ne primenjuje na anonimizovane podatke. Lična kontrola nad obradom sopstvenih podataka i svest o njoj ključne su za analitiku velikih podataka. Bez njih nije moguće sa sigurnošću znati ko je rukovalac podacima, a ko obrađivač podataka, čime se onemogućava efikasno ostvarivanje ličnih prava.

1013 *Ibid.*, str. 2.

10.2. Tehnologije Web 2.0 i 3.0: društvene mreže i internet stvari

Ključne tačke

- Usluge socijalnog umrežavanja (engl. *Social Networking Services*, SNS) mrežne su platforme za komunikaciju koje pojedincima omogućavaju da se pridružuju mrežama istomišljenika ili da ih stvaraju.
- Internet stvari (engl. *Internet of Things*) predstavlja povezivanje objekata s internetom, te međupovezivanje tih objekata.
- Pristanak ispitanika najčešća je pravna osnova za zakonitu obradu podataka koju rukovaoci podacima provode na društvenim mrežama.
- Korisnici društvenih mreža uglavnom su zaštićeni „izuzećem za domaćinstvo", ali to odstupanje se može ukinuti u određenim kontekstima.
- Pružaoci usluga društvenih mreža nisu zaštićeni „izuzećem za domaćinstvo".
- Tehnička i integrisana zaštita podataka ključne su za obezbeđivanjem sigurnosti podataka u toj oblasti.

10.2.1. Definisanje tehnologija Web 2.0 i 3.0

Usluge socijalnog umrežavanja

Internet je prvobitno zamišljen kao mreža za povezivanje računara i prenošenje poruka s ograničenim mogućnostima razmene podataka, a internet stranice trebalo je da pojedincima pruže tek mogućnost pasivnog pregleda njihovog sadržaja[1014]. U doba tehnologije Web 2.0 internet je pretvoren u forum u sklopu kojeg korisnici mogu da komuniciraju, sarađuju i stvaraju sadržaj. Ovaj period je obeležio neverovatan uspeh i raširena upotreba usluga socijalnog umrežavanja, koje su sada neizostavan deo svakodnevnog života miliona ljudi.

Usluge socijalnog umrežavanja (SNS) ili „društvene mreže" generalno mogu da se definišu kao „mrežne platforme za komunikaciju koje pojedincima omogućavaju

1014 Evropska komisija (2016), *Postizanje napretka u pogledu interneta stvari u Evropi*, SWD(2016) 110 final.

da se pridružuju mrežama istomišljenika ili ih stvaraju"[1015]. Da bi stvorili mrežu ili joj se pridružili, pojedinci treba da pruže lične podatke i izrade profil. SNS omogućava korisnicima stvaranje digitalnog „sadržaja", koji obuhvata fotografije, video-zapise, linkove za novinske članke i lične objave u kojima izražavaju mišljenje. Putem tih mrežnih platformi za komunikaciju korisnici mogu da ostvare kontakt i komuniciraju sa nekoliko drugih korisnika. Važna je činjenica da većina popularnih SNS-ova ne zahteva nikakve naknade za registraciju. Umesto obavezivanja korisnika da plate za pridruživanje mreži, pružaoci SNS-ova većinu prihoda ostvaruju od ciljanog oglašavanja. Oglašivači mogu da ostvare veliku korist od ličnih podataka koji se svakodnevno otkrivaju na tim internet stranicama. Informacije o uzrastu, polu, lokaciji i interesima korisnika omogućavaju da njihovi oglasi dopru do „odgovarajućih" ljudi.

Komitet ministara Saveta Evrope usvojio je Preporuku o zaštiti ljudskih prava u vezi s uslugama društvenog umrežavanja (dostupnu na engleskom jeziku)[1016], čiji se jedan deo odnosi posebno na zaštitu podataka, pa je 2018. dopunjena Preporukom o ulogama i odgovornostima internet posrednika[1017].

Primer: Nora je veoma srećna jer ju je njen partner zaprosio. Želi da podeli tu srećnu vest sa porodicom i prijateljima, pa odlučuje da napiše emotivnu objavu na društvenoj mreži u kojoj izražava svoju radost i menja status veze u „verena". Sledećih nekoliko dana prilikom prijave na profil Nori se prikazuju oglasi o venčanicama i cvećarama. Zašto se to dešava?

Kada stvaraju oglase na Facebooku, firme koje se bave prodajom venčanica i cveća biraju određene parametre kako bi mogle da dopru do osoba kao što je Nora. Kada Norin profil pokazuje da je ona žena, verena i živi u Parizu, u blizini oblasti u kojima se nalaze saloni venčanica i cvećare koje prikazuju oglase, Nori odmah počinju da se prikazuju ti oglasi.

1015 Radna grupa iz člana 29. (2009), *Mišljenje 5/2009 o društvenim mrežama na internetu*, WP 163, 12. juna 2009., str. 4.

1016 Savet Evrope, Komitet ministara, Preporuka CM/Rec(2012)4 Odbora ministara državama članicama o zaštiti ljudskih prava u vezi s uslugama društvenog umrežavanja, 4. aprila 2012.

1017 Savet Evrope, Komitet ministara, Preporuka CM/Rec(2018)2 Odbora ministara državama članicama o ulogama i odgovornostima internet posrednika, 7. marta 2018.

Internet stvari

Internet stvari (IoT) predstavlja sledeći korak u razvoju interneta: razdoblje tehnologije Web 3.0. Uz pomoć IoT-a uređaji mogu da se povežu i komuniciraju s drugim uređajima putem interneta. To omogućava da se objekti i osobe međusobno povežu putem komunikacionih mreža i izveštavaju o svom statusu i/ili o statusu okruženja[1018]. IoT i povezani uređaji već su postali stvarnost i očekuje se da će nastaviti znatno da rastu u dolazećim godinama i da će se stvoriti i dodatno razviti pametni uređaji koji će dovesti do stvaranja pametnih gradova, pametnih domova i pametnih preduzeća.

Primer: IoT može biti posebno koristan za zdravstvo. Kompanije su već izradile uređaje, senzore i aplikacije koje omogućavaju praćenje zdravlja pacijenata. Upotrebom nosivog dugmeta za alarm i drugih bežičnih senzora koji se postavljaju u domu moguće je pratiti svakodnevne navike starijih osoba koje žive same i slati upozorenja ako dođe do većih promena njihovog dnevnog rasporeda. Na primer, starije osobe često upotrebljavaju senzore pada. Ti senzori mogu precizno da otkriju padove i obaveste lekara i/ili porodicu te osobe o njenom padu.

Primer: Barselona je jedan od najpoznatijih primera pametnog grada. Grad od 2012. godine uvodi inovativne tehnologije čiji je cilj da se stvori pametan sistem javnog prevoza, zbrinjavanja otpada, parkiranja i ulične rasvete. Na primer, kako bi se poboljšalo uklanjanje otpada, u gradu se upotrebljavaju pametne kante za otpad. One omogućavaju praćenje nivoa otpada radi optimizacije ruta za njegovo prikupljanje. Kada su kante gotovo pune, šalju signale putem mobilne komunikacione mreže, koji se šalju softverskoj aplikaciji koju upotrebljava preduzeće za zbrinjavanje otpada. Preduzeće tako može da isplanira najbolju rutu za prikupljanje otpada, određuje prioritete i/ili organizuje preuzimanje samo onih kanti koje treba isprazniti.

10.2.2. Procena koristi i rizika

Snažno širenje i velik uspeh SNS-ova u protekloj deceniji ukazuju na to da oni donose **značajne koristi**. Na primer, ciljano oglašavanje (opisano u istaknutom pri-

1018 Evropska komisija, Radni dokument službi Komisije, *Postizanje napretka u pogledu interneta stvari u Evropi*, SWD(2016) 110, 19. aprila 2016.

meru) posebno je inovativan način na koji preduzeća mogu dopreti do potrošača i prodreti na specifično tržište. Takođe bi moglo biti u interesu potrošača da im se prikazuju oglasi koji su im relevantniji i zanimljiviji. Važno je istaknuti i da usluge socijalnog umrežavanja i društvene mreže mogu da imaju pozitivan efekat na društvo i uvođenje promena. One korisnicima omogućavaju komunikaciju, interakciju i organizovanje grupa i događaja u vezi sa temama koje utiču na njih.

Isto tako, očekuje se da IoT pruži znatne koristi ekonomiji, pa je deo strategije EU za razvoj jedinstvenog digitalnog tržišta. Procenjuje se da će u EU tokom 2020. broj veza u sklopu IoT-a narasti na šest milijardi. Očekuje se da će širenje povezanosti doneti važne ekonomske koristi zahvaljujući razvoju inovativnih usluga i aplikacija, boljeg zdravstva, boljeg razumevanja potreba potrošača i povećane efikasnosti.

S druge strane, s obzirom na to da korisnici društvenih mreža stvaraju velike količine ličnih podataka koje zatim operatori usluga obrađuju, uz širenje SNS-ova veže se **sve veća zabrinutost** oko načina na koji se privatnost i lični podaci mogu zaštititi. SNS-ovi mogu ugroziti pravo na privatni život i pravo na slobodu izražavanja. Mogu se javiti sledeće pretnje: „izostanak zakonskih i procesnih zaštitnih mera za procese koji mogu dovesti do isključenosti korisnika; neodgovarajuća zaštita dece i mladih od štetnog sadržaja ili ponašanja; manjak poštovanja za prava drugih; manjak zadatih postavki koje omogućavaju privatnost; manjak transparentnosti u vezi sa svrhama u koje se lični podaci prikupljaju i obrađuju“[1019]. Evropskim pravom zaštite podataka nastoji se da se suprotstavi izazovima zaštite privatnosti/podataka koje nose društvene mreže. Načela pristanka, tehničke i integrisane zaštite privatnosti/podataka i prava pojedinaca posebno su važna u kontekstu društvenih mreža i usluga umrežavanja.

U kontekstu IoT-a veoma velika količina ličnih podataka koji nastaju na različitim međusobno povezanim uređajima takođe uključuje rizike za privatnost i zaštitu podataka. Iako je transparentnost važno načelo evropskog zakonodavstva o zaštiti podataka, zbog velikog broja povezanih uređaja nije uvek jasno ko može da pristupa podacima prikupljenima s uređaja iz mreže IoT-a i da ih prikuplja i upotrebljava[1020]. Međutim, u skladu sa pravom Unije i Saveta Evrope, načelom transparentnosti uslovljava se obaveza rukovaoca podacima da jasnim i razumljivim jezikom obaveštava ispitanike o načinu upotrebe njihovih podataka. Rizici, pravila, zaštitne mere i prava u

1019 Savet Evrope, Preporuka Rec(2012)4 državama članicama o zaštiti ljudskih prava u vezi s uslugama društvenog umrežavanja, 4. aprila 2012.

1020 Evropski nadzornik za zaštitu podataka (2017.), *Understanding the Internet of Things* (Razumevanje interneta stvari).

pogledu obrade njihovih ličnih podataka moraju da budu jasni dotičnim pojedincima. Uređaji povezani putem IoT-a i brojni postupci obrade i predmetni podaci takođe mogu da dovedu u pitanje zahtev davanja jasnog pristanka utemeljenog na informacijama za obradu podataka, u slučajevima u kojima je takva obrada zasnovana na pristanku. Pojedinci često nedovoljno razumeju tehnički aspekt takve obrade, a time i posledice davanja pristanka.

Drugo važno pitanje je bezbednost, budući da su povezani uređaji posebno izloženi bezbednosnim rizicima. Povezani uređaji imaju različite nivoe zaštite. Budući da se upotrebljavaju izvan standardne informatičke infrastrukture, mogu im nedostajati odgovarajuća procesorska snaga i kapacitet za čuvanje podataka, koji su potrebni za instaliranje softvera ili primenu metoda kao što su šifrovanje, pseudonimizacija ili anonimizacija radi zaštite ličnih podataka korisnika.

Primer: Nemački zakonodavci su odlučili da uvedu zabranu igračke koja se povezuje s internetom pošto je iznesena zabrinutost u vezi s uticajem igračke na poštovanje privatnog života dece. Zaključili su da lutka po imenu Kajla, koja se povezuje s internetom, zapravo predstavlja prikriveni uređaj za špijuniranje. Lutka je slala zvučna pitanja koje je dete postavljalo tokom igre aplikaciji na digitalnom uređaju, koja ih je pretvarala u tekst i zatim tražila odgovor putem interneta. Aplikacija bi zatim poslala odgovor lutki, koja bi ga izgovorila detetu. Tom lutkom bi mogla da se snima komunikacija deteta, kao i odraslih osoba u blizini, i da se pošalje aplikaciji. Da proizvođači lutke nisu primenili odgovarajuće sigurnosne mere, lutku je neko mogao da upotrebi za prisluškivanje razgovora.

10.2.3. Problemi u vezi sa zaštitom podataka

Pristanak

U Evropi je obrada ličnih podataka zakonita samo ako je dozvoljena evropskim pravom zaštite podataka. Za pružaoce SNS-ova pristanak ispitanika uglavnom predstavlja zakonitu osnovu za obradu podataka. Pristanak mora da bude dobrovoljno dat, poseban, zasnovan na informacijama i nedvosmislen (videti deo 4.1.1)[1021]. „Dobrovoljno dat" u osnovi znači da ispitanici moraju da imaju mogućnost stvarnog izbora. Pristanak je „poseban" i „utemeljen na informacijama" kada je razumljiv i jasno i precizno upućuje na celovit opseg, svrhe i posledice obrade podataka. U kontek-

1021 Opšta uredba o zaštiti podataka, članovi 4. i 7.; modernizovana Konvencija br. 108, član 5.

stu društvenih mreža može biti upitno da li je pristanak dobrovoljno dat, poseban i utemeljen na informacijama za sve vrste obrade koje vrše operator SNS-a i treće strane.

Primer: Za pridruživanje i pristup SNS-u pojedinci često moraju da pristanu na različite vrste obrade svojih ličnih podataka, i to bez potrebnih konkretnih informacija ili drugih mogućnosti. Primer je potreba davanja pristanka za dobijanje bihevioralnih oglasa radi registracije u SNS. Kako navodi Radna grupa iz člana 29. u svom Mišljenju o definiciji pristanka, „s obzirom na važnost koju su neke društvene mreže stekle, određene kategorije korisnika (poput tinejdžera) prihvatiće dobijanje bihevioralnih oglasa kako bi izbegle rizik od delimičnog isključivanja iz društvene interakcije. Korisnik bi trebalo da bude u poziciji da dâ dobrovoljan i poseban pristanak za dobijanje bihevioralnih oglasa, nezavisno od njegovog pristupa usluzi socijalnog umrežavanja"[1022].

Prema Opštoj uredbi o zaštiti podataka, lični podaci dece mlađe od 16 godina u načelu se ne smeju obrađivati na osnovu njihovog pristanka[1023]. Ako je za obradu potreban pristanak, mora je dati roditelj ili staratelj deteta. Deci je potrebna posebna zaštita zbog toga što mogu da budu manje svesna rizika i posledica obrade podataka. To je vrlo važno u kontekstu društvenih mreža jer su deca izloženija određenim negativnim efektima koji se mogu javiti prilikom njihove upotrebe, poput virtualnog zlostavljanja (engl. *cyberbullying*), uhođenja putem interneta ili krađe identiteta.

Bezbednost i tehnička i integrisana zaštita privatnosti/podataka

Obrada ličnih podataka nosi određene neizbežne bezbednosne rizike s obzirom da postoji neprestana mogućnost povrede bezbednosti koja vodi do nehotičnog ili nezakonitog uništenja, gubitka, izmene ili otkrivanja obrađenih ličnih podataka ili neovlašćenog pristupa njima. Prema evropskom pravu zaštite podataka, rukovaoci podacima i obrađivači podataka obavezni su da izvrše odgovarajuće tehničke i organizacione mere kako bi sprečili neovlašćeno ometanje postupaka obrade podataka. Pružaoci usluga socijalnog umrežavanja, koji podležu evropskim propisima o zaštiti podataka, takođe moraju da poštuju tu obavezu.

1022 Radna grupa iz člana 29. (2011), *Mišljenje 15/2011 o definiciji pristanka*, WP 187, 13. jula 2011., str. 18.

1023 Vidi Opštu uredbu o zaštiti podataka, član 8. Države članice EU mogu zakonom propisati nižu uzrasnu granicu, pod uslovom da ona nije niža od 13 godina.

Prema načelima tehničke i integrisane zaštite privatnosti/podataka od rukovaoca podacima zahteva se da održavaju bezbednost tehničke izrade svojih proizvoda i automatski primenjuju odgovarajuće postavke privatnosti i zaštite podataka. To znači da kada neka osoba odluči da se pridruži društvenoj mreži, pružalac usluga ne mora automatski da dâ sve informacije o novom korisniku usluge svim svojim korisnicima. Prilikom priključivanja na uslugu zadate postavke privatnosti i zaštite podataka treba da budu takve da su informacije dostupne samo odabranim kontaktima te osobe. Omogućavanje pristupa osobama izvan tog popisa trebalo bi da bude moguće tek pošto korisnik ručno promeni zadate postavke privatnosti i zaštite podataka. To može imati uticaja i u slučajevima u kojima dođe do povrede podataka uprkos uspostavljenim sigurnosnim merama. U takvim slučajevima pružaoci usluga moraju da obaveste dotične korisnike ako postoji verovatnoća da će doći do visokog rizika za prava i slobode ispitanika[1024].

Tehnička i integrisana zaštita privatnosti/podataka posebno su važne u kontekstu SNS-ova budući da, povrh rizika od neovlašćenog pristupa koje nosi većina vrsta obrade, i deljenje ličnih podataka na društvenim mrežama uzrokuje dodatne bezbednosne rizike. Oni su obično uzrokovani nedovoljnim razumevanjem pojedinaca u pogledu toga *ko* može da pristupa njihovim informacijama i kako može da ih upotrebljava. Kako raste raširenost upotrebe društvenih mreža, tako raste i broj incidenata krađe identiteta i njenih žrtava.

Primer: Krađa identiteta je pojava do koje dolazi kada jedna osoba dođe do informacija, podataka ili dokumenata koji pripadaju drugoj osobi (žrtvi) i zatim upotrebljava te podatke da bi se lažno predstavljala kao žrtva i dobijala proizvode i usluge u njeno ime. Na primer, Pol ima korisnički račun na internet stranici jedne društvene mreže. Pol je nastavnik i aktivan član svoje zajednice, vrlo je druželjubiv i nije preterano zabrinut oko postavki privatnosti i zaštite podataka na svom profilu na društvenoj mreži. Ima dugu listu kontakata, koji ponekad uključuju i osobe koje ne poznaje nužno lično. Budući da je zaposlen u velikoj školi i vrlo je popularan kao trener školskog fudbalskog tima, veruje da su ti ljudi najverovatnije roditelji ili prijatelji osoba koje rade u školi ili je pohađaju. Polova adresa e-pošte i datum rođenja vidljivi su na njegovom profilu na društvenoj mreži. Osim toga, Pol redovno objavljuje fotografije svog psa Tobija, uz podnaslove poput „Tobi i ja u jutarnjoj šetnji". Pol nije svestan da je jedno od najpopularnijih bezbednosnih pitanja za zaštitu profila e-pošte ili

1024 *Ibid.*, član 34.

mobilnog telefona „kako se zove vaš kućni ljubimac". Upotrebom informacija koje su dostupne na Polovom profilu na društvenoj mreži Nik jednostavno uspeva da hakuje Polove račune.

Prava pojedinaca

Pružaoci SNS-ova moraju poštovati prava pojedinaca (videti deo 6.1), uključujući pravo na informacije o svrsi obrade i načinu upotrebe ličnih podataka u svrhe direktnog marketinga. Pojedincima se takođe mora obezbediti pravo na pristup ličnim podacima koje su stvorili u okviru platforme društvene mreže i na zahtev za njihovo brisanje. Čak i kada osobe pristanu na obradu ličnih podataka i učitaju podatke na mrežu, trebalo bi da imaju mogućnost da zatraže da „budu zaboravljene" ako više ne žele usluge te društvene mreže. Pravom na prenosivost podataka korisnicima se dodatno omogućava primanje kopije ličnih podataka koje daju pružaocu usluga socijalnog umrežavanja u strukturiranom, uobičajeno upotrebljavanom i mašinski čitljivom formatu i prenošenje sopstvenih podataka od jednog pružaoca usluga socijalnog umrežavanja drugom[1025].

Rukovaoci podacima

Teško pitanje koje se često postavlja u kontekstu društvenih mreža jeste ko je rukovalac podacima, odnosno ko je osoba koja ima obavezu i odgovornost da se pridržava propisa o zaštiti podataka. Pružaoci usluga socijalnog umrežavanja smatraju se rukovaocima podacima u skladu sa evropskim zakonodavstvom o zaštiti podataka. To je vidljivo prema širokoj definiciji pojma „rukovaoca podacima" i činjenici da ti pružaoci usluga određuju svrhu i sredstva obrade ličnih podataka koje dele pojedinci. U skladu sa pravom EU, ako pružaju usluge ispitanicima u EU, rukovaoci podacima moraju da se pridržavaju odredbi Opšte uredbe o zaštiti podataka, čak i ako nemaju sedište u EU.

Međutim, da li mogu i korisnici usluga socijalnog umrežavanja da se smatraju rukovaocima podacima? Ako pojedinci obrađuju lične podatke „tokom isključivo ličnih ili kućnih aktivnosti", propisi o zaštiti podataka se ne primenjuju. To je u evropskom pravu zaštite podataka poznato kao „izuzeće za domaćinstvo". Međutim, u nekim slučajevima korisnik usluge socijalnog umrežavanja možda nije obuhvaćen izuzećem za domaćinstvo.

1025 Opšta uredba o zaštiti podataka, član 21.

Korisnici dobrovoljno dele svoje lične podatke na mreži. Međutim, informacije koje se dele na mreži često uključuju lične podatke drugih osoba.

Primer: Pol ima korisnički račun na vrlo popularnoj platformi društvene mreže. Pol pokušava da postane glumac i služi se nalogom da bi objavljivao fotografije, video-zapise i objave u kojima objašnjava svoju strast prema umetnosti. Popularnost je važna za njegovu budućnost i zato odlučuje da bi njegov profil trebalo da bude dostupan ne samo uskom krugu njegovih kontakata, nego svim korisnicima interneta, nezavisno od toga da li su članovi mreže. Da li Pol sme da objavljuje fotografije i video-zapise sebe i svoje prijateljice Sare bez njenog pristanka? Sara je učiteljica nižih razreda osnovne škole, pa nastoji da čuva svoj privatni život podalje od poslodavca, svojih učenika i njihovih roditelja. Zamislite slučaj u kojem Sara, koja se ne služi društvenim mrežama, sazna od zajedničkog prijatelja Nicka da je fotografija nje i Pola na zabavi objavljena na internetu. U takvom slučaju Polova obrada podataka ne potpada pod pravo Unije, jer je obuhvaćena „izuzećem za domaćinstvo".

Međutim, neophodno je da korisnici budu svesni i imaju na umu da učitavanje podataka o drugim osobama bez njihovog pristanka može uzrokovati povredu prava na privatnost i zaštitu podataka tih osoba. Čak i kada se primenjuje izuzeće za domaćinstvo, na primer ako korisnik ima profil koji je dostupan samo popisu kontakata koje on odabere, taj korisnik bi i dalje mogao da snosi odgovornost za objavu ličnih podataka o drugima. Iako se propisi o zaštiti podataka ne primenjuju ako se primenjuje izuzeće za domaćinstvo, odgovornost može proizlaziti iz primene drugih domaćih propisa, na primer u slučaju klevete i povrede prava ličnosti. Konačno, izuzećem za domaćinstvo zaštićeni su samo korisnici SNS-ova: rukovaoci podacima i obrađivači podataka koji pružaju sredstva za takvu privatnu obradu obuhvaćeni su pravom zaštite podataka EU[1026].

Nakon izmene Direktive o privatnosti i elektronskim komunikacijama, propisi o zaštiti podataka, privatnosti i bezbednosti koji se primenjuju na pružaoce telekomunikacionih usluga u sklopu postojećeg pravnog okvira primenjivali bi se i na usluge komunikacije među uređajima i elektronske komunikacione usluge, uključujući, na primer, OTT usluge.

1026 *Ibid.*, uvodna izjava 18.

Dodatna literatura

Poglavlje 1.

Araceli Mangas, M. (ed.) (2008), *Carta de los derechos fundamentales de la Unión Europea*, Bilbao, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit*, Beč, Manz'sche Verlags- und Universitätsbuchhandlung.

Docksey, C. „Four fundamental rights: finding the balance", *International Data Privacy Law*, sv. 6, br. 3, str. 195–209.

EDRi, *An introduction to data protection*, Bruxelles.

Frowein, J. i Peukert, W. (2009.), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

González Fuster, G. i Gellert, G. (2012), „The fundamental right of data protection in the European Union: in search of an uncharted right", *International Review of Law, Computers and Technology*, sv. 26 (1), str. 73–82.

Grabenwarter, C. i Pabel, K. (2012), *Europäische Menschenrechtskonvention*, München, C. H. Beck.

Gutwirth, S., Poullet, Y., de Hert, P., de Terwange, C. i Nouwt, S. (Eds.) (2009), *Reinventing Data Protection*, Springer.

Harris, D., O'Boyle, M., Warbrick, C. i Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Hijmans, H. (2016), *The European Union as Guardian of Internet Privacy – the Story of Art 16 TFEU*, Springer.

Hustinx, P. (2016), „EU Data Protection Law: the review of Directive 95/46/EC and the Proposed General Data Protection Regulation".

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, München, C. H. Beck.

Kokott, J. i Sobotta, C. (2013), „The distinction between privacy and data protection in the case law of the CJEU and the ECtHR", *International Data Privacy Law*, sv. 3, br. 4, str. 222–228.

Kranenborg, H. (2015), „Google and the Right to be Forgotten", *European Data Protection Law Review*, sv. 1, br. 1, str. 70–79.

Lynskey, O. (2014), „Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order", *International and Comparative Law Quarterly*, sv. 63, br. 3, str. 569–597.

Lynskey, O. (2015), *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights*, Oxford, Oxford University Press.

Nowak, M., Januszewski, K. i Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antwerpen, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. i Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Bruxelles, Emile Bruylant.

Simitis, S. (1997), „Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?", *Neue Juristische Wochenschrift*, br. 5, str. 281–288.

Warren, S. i Brandeis, L. (1890), „The right to privacy", *Harvard Law Review,* sv. 4, br. 5, str. 193–220.

White, R. i Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Poglavlje 2.

Acquisty, A. i Gross R. (2009), „Predicting Social Security numbers from public data", *Proceedings of the National Academy of Science*, 7. jula 2009.

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M. i Blondel V. D. (2013.), „Unique in the Crowd: the Privacy Bounds of Human Mobility", *Nature Scientific Reports*, sv. 3, 2013.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Pariz, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

González Fuster, G. (2014), *The Emergence of Personal Data Protection as a Fundamental Right in the EU*, Springer.

Morgan, R. i Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, London, Sweet & Maxwell.

Ohm, P. (2010), „Broken promises of privacy: Responding to the surprising failure of anonymization", *UCLA Law Review*, sv. 57, br. 6, str. 1701–1777.

Samarati, P. i Sweeney, L. (1998), „Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression", tehničko izveštaj SRI-CSL-98-04.

Sweeney, L. (2002), „K-Anonymity: A Model for Protecting Privacy" *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, sv. 10, br. 5, str. 557.–570.

Tinnefeld, M., Buchner, B. i Petri, T. (2012.), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, München, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), Anonymisation: managing data protection risk. *Code of practice*.

Poglavlja od 3. do 6.

Brühann, U. (2012), „Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" u: Grabitz, E., Hilf, M. i Nettesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, München, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cadiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrücken, Éditions universitaires européennes.

Curren, L. i Kaye, J. (2010), „Revoking consent: a 'blind spot' in data protection law?", *Computer Law & Security Review*, sv. 26, br. 3, str. 273–283.

Dammann, U. i Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

De Hert, P. i Papakonstantinou, V. (2012), „The Police and Criminal Justice Data Protection Directive: Comment and Analysis", *Computers & Law Magazine of SCL*, sv. 22, br. 6, str. 1–5.

De Hert, P. i Papakonstantinou, V. (2012), „The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *Computer Law & Security Review*, sv. 28, br. 2, str. 130–142.

Feretti, Federico (2012), „A European perspective on data processing consent through the re-conceptualization of European data protection's looking glass after the Lisbon treaty: Taking rights seriously", *European Review of Private Law*, sv. 20, br. 2, str. 473–506.

FRA (Agencija Evropske unije za osnovna prava) (2010), *Data Protection in the European Union: the role of National Supervisory authorities (Strengthening the fundamental rights architecture in the EU II),* Luksemburg, Kancelarija za publikacije Evropske unije (Kancelarija za publikacije).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (konferencijsko izdanje), Beč, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luksemburg, Kancelarija za publikacije.

Irish Health Information and Quality Authority (2010), Guidance on Privacy Impact Assessment in Health and Social Care.

Kierkegaard, S., Waters, N., Greenleaf, G., Bygrave, L. A., Lloyd, I. i Saxby, S. (2011), „30 years on – The review of the Council of Europe Data Protection Convention 108", *Computer Law & Security Review*, sv. 27, br. 3, str. 223–231.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, Privacy Impact Assessment.

Poglavlje 7.

Evropski nadzornik za zaštitu podataka (2014), Position paper on transfer of personal data to third countries and international organisations by EU institutions and bodies.

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. i Nouwt, S. (2009), *Reinventing data protection?*, Berlin, Springer.

Kuner, C. (2007), *European data protection law*, Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press.

Radna grupa iz člana 29 (2005), *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*.

Poglavlje 8.

Blasi Casagran, C. (2016) *Global Data Protection in the Field of Law Enforcement, an EU Perspective*, London, Routledge.

Boehm, F. (2012), *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level,* Berlin, Springer.

De Hert, P. i Papakonstantinou, V. (2012), *„The Police and Criminal Justice Data Protection Directive: Comment and Analysis"*, *Computers & Law Magazine of SCL*, sv. 22, br. 6, str. 1–5.

Drewer, D., Ellermann, J. (2012), „Europol's data protection framework as an asset in the fight against cybercrime"*, ERA Forum*, sv. 13, br. 3, str. 381–395.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, Haag, Eurojust.

Europol (2012), *Data Protection at Europol*, Luksemburg, Kancelarija za publikacije.

Gutiérrez Zarza, A. (2015), *Exchange of Information and Data Protection in Cross--border Criminal Proceedings in Europe*, Berlin, Springer.

Gutwirth, S., Poullet, Y. i De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. i Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), „Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem", *European Law Review*, sv. 36, br. 5, str. 722–776.

Santos Vara, J. (2013), *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, Centre for the Law of External Relations, CLEER, radni dokumenti 2013/2.

Poglavlje 9.

Büllesbach, A., Gijrath, S., Poullet, Y. i Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. i Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. i De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. i Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), „Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem", *European Law Review*, sv. 36, br. 5, str. 722–776.

Rosemary, J. i Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.

Poglavlje 10.

El Emam, K. i Álvarez, C. (2015), „A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques", *International Data Privacy Law*, sv. 5, br. 1, str. 73–87.

Mayer-Schönberger, V. i Cate, F. (2013), „Notice and consent in a world of Big Data", *International Data Privacy Law*, sv. 3, br. 2, str. 67–73.

Rubistein, I. (2013), „Big Data: The End of Privacy or a New Beginning?", *International Data Privacy Law*, sv. 3, br. 2, str. 74–87.

Sudska praksa

Odabrana sudska praksa Evropskog suda za ljudska prava

Pristup ličnim podacima

Gaskin protiv Ujedinjenog Kraljevstva, br. 10454/83, 7. jula 1989.

Godelli protiv Italije, br. 33783/09, 25. septembra 2012.

K. H. i drugi protiv Slovačke, br. 32881/04, 28. aprila 2009.

Leander protiv Švedske, br. 9248/81, 26. marta 1987.

M. K. protiv Francuske, br. 19522/09, 18. aprila 2013.

Odièvre protiv Francuske [VV], br. 42326/98, 13. februara 2003.

Procena zaštite podataka, slobode izražavanja i prava na informacije

Axel Springer AG protiv Nemačke [VV], br. 39954/08, 7. februara 2012.

Bohlen protiv Nemačke, br. 53495/09, 19. februara 2015.

Coudec i Hachette Filipacchi Associés protiv Francuske [VV], br. 40454/07, 10. novembra 2015.

Magyar Helsinki Bizottság protiv Mađarske [VV], br. 18030/11, 8. novembra 2016.

Müller i drugi protiv Švajcarske, br. 10737/84, 24. maja 1988.

Satakunnan Markkinapörssi Oy i Satamedia Oy protiv Finske [VV], br. 931/13, 27. juna 2017.

Vereinigung bildender Künstler protiv Austrije, br. 68354/01, 25. januara 2007.

Von Hannover protiv Nemačke (br. 2) [VV], br. 40660/08 i 60641/08, 7. februara 2012.

Procena zaštite podataka i slobode veroispovesti

Sinan Işık protiv Turske, br. 21924/05, 2. februara 2010.

Izazovi mrežne zaštite podataka

K. U. protiv Finske, br. 2872/02, 2. decembra 2008.

Pristanak/saglasnost ispitanika

Elberte protiv Letonije, br. 61243/08, 13. januara 2015.

Sinan Işık protiv Turske, br. 21924/05, 2. februara 2010.

Y. protiv Turske, br. 648/10, 17. februara 2015.

Prepiska

Amann protiv Švajcarske [VV], br. 27798/95, 16. februara 2000.

Bernh Larsen Holding AS i drugi protiv Norveške, br. 24117/08, 14. marta 2013.

Cemalettin Canli protiv Turske, br. 22427/04, 18. novembra 2008.

D. L. protiv Bugarske, br. 7472/14, 19. maja 2016.

Dalea protiv Francuske, br. 964/07, 2. februara 2010.

Gaskin protiv Ujedinjenog Kraljevstva, br. 10454/83, 7. jula 1989.

Haralambie protiv Rumunije, br. 21737/03, 27. oktobra 2009.

Khelili protiv Švajcarske, br. 16188/07, 18. oktobra 2011.

Leander protiv Švedske, br. 9248/81, 26. marta 1987.

Malone protiv Ujedinjenog Kraljevstva, br. 8691/79, 2. avgusta 1984.

Rotaru protiv Rumunije [VV], br. 28341/95, 4. maja 2000.

S. i Marper protiv Ujedinjenog Kraljevstva [VV], br. 30562/04 i 30566/04, 4. decembra 2008.

Shimovolos protiv Rusije, br. 30194/09, 21. juna 2011.

Silver i drugi protiv Ujedinjenog Kraljevstva, br. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. marta 1983.

Sunday Times protiv Ujedinjenog Kraljevstva, br. 6538/74, 26. aprila 1979.

Udruženje za evropsku integraciju i ljudska prava i Ekimdzhiev protiv Bugarske, br. 62540/00, 28. juna 2007.

Baze podataka o krivičnim evidencijama

Aycaguer protiv Francuske, br. 8806/12, 22. juna 2017.
B. B. protiv Francuske, br. 5335/06, 17. decembra 2009.
Brunet protiv Francuske, br. 21010/10, 18. septembra 2014.
M. K. protiv Francuske, br. 19522/09, 18. aprila 2013.
M. M. protiv Ujedinjenog Kraljevstva, br. 24029/07, 13. novembra 2012.

Bezbednost podataka

Haralambie protiv Rumunije, br. 21737/03, 27. oktobra 2009.
K. H. i drugi protiv Slovačke, br. 32881/04, 28. aprila 2009.

Baze podataka o DNK

S. i Marper protiv Ujedinjenog Kraljevstva [VV], br. 30562/04 i 30566/04, 4. decembra 2008.

Podaci GPS-a

Uzun protiv Nemačke, br. 35623/05, 2. septembra 2010.

Zdravstveni podaci

Avilkina i drugi protiv Rusije, br. 1585/09, 6. juna 2013.
Biriuk protiv Litvanije, br. 23373/03, 25. novembra 2008.
I. protiv Finske, br. 20511/03, 17. jula 2008.
L. H. protiv Latvije, br. 52019/07, 29. aprila 2014.
L. L. protiv Francuske, br. 7508/02, 10. oktobra 2006.
M. S. protiv Švedske, br. 20837/92, 27. avgusta 1997.
Szuluk protiv Ujedinjenog Kraljevstva, br. 36936/05, 2. juna 2009.
Y. protiv Turske, br. 648/10, 17. februara 2015.
Z. protiv Finske, br. 22009/93, 25. februara 1997.

Identitet

Ciubotaru protiv Moldavije, br. 27138/04, 27. aprila 2010.
Godelli protiv Italije, br. 33783/09, 25. septembra 2012.
Odièvre protiv Francuske [VV], br. 42326/98, 13. februara 2003.

Informacije o profesionalnim delatnostima

G. S. B. protiv Švajcarske, br. 28601/11, 22. decembra 2015.
M. N. i drugi protiv San Marina, br. 28005/12, 7. jula 2015.
Michaud protiv Francuske, br. 12323/11, 6. decembra 2012.
Niemietz protiv Nemačke, br. 13710/88, 16. decembra 1992.

Presretanje komunikacije

Amann protiv Švajcarske [VV], br. 27798/95, 16. februara 2000.
Brito Ferrinho Bexiga Villa-Nova protiv Portugalije, br. 69436/10, 1. decembra 2015.
Copland protiv Ujedinjenog Kraljevstva, br. 62617/00, 3. aprila 2007.
Halford protiv Ujedinjenog Kraljevstva, br. 20605/92, 25. juna 1997.
Iordachi i drugi protiv Moldavije, br. 25198/02, 10. februara 2009.
Kopp protiv Švajcarske, br. 23224/94, 25. marta 1998.
Liberty i drugi protiv Ujedinjenog Kraljevstva, br. 58243/00, 1. jula 2008.
Malone protiv Ujedinjenog Kraljevstva, br. 8691/79, 2. avgusta 1984.
Mustafa Sezgin Tanrıkulu protiv Turske, br. 27473/06, 18. jula 2017.
Pruteanu protiv Rumunije, br. 30181/05, 3. februara 2015.
Szuluk protiv Ujedinjenog Kraljevstva, br. 36936/05, 2. juna 2009.

Obaveze nosilaca dužnosti

B. B. protiv Francuske, br. 5335/06, 17. decembra 2009.
I. protiv Finske, br. 20511/03, 17. jula 2008.
Mosley protiv Ujedinjenog Kraljevstva, br. 48009/08, 10. maja 2011.

Lični podaci

Amann protiv Švajcarske [VV], br. 27798/95, 16. februara 2000.
Bernh Larsen Holding AS i drugi protiv Norveške, br. 24117/08, 14. marta 2013.
Uzun protiv Nemačke, br. 35623/05, 2010.

Fotografije

Sciacca protiv Italije, br. 50774/99, 11. januara 2005.
Von Hannover protiv Nemačke, br. 59320/00, 24. juna 2004.

Pravo na zaborav

Satakunnan Markkinapörssi Oy i Satamedia Oy protiv Finske [VV], br. 931/13, 27. juna 2017.

Segerstedt-Wiberg i drugi protiv Švedske, br. 62332/00, 6. juna 2006.

Pravo na prigovor

Leander protiv Švedske, br. 9248/81, 26. marta 1987.

M. S. protiv Švedske, br. 20837/92, 27. avgusta 1997.

Mosley protiv Ujedinjenog Kraljevstva, br. 48009/08, 10. maja 2011.

Rotaru protiv Rumunije [VV], br. 28341/95, 4. maja 2000.

Sinan Işık protiv Turske, br. 21924/05, 2. februara 2010.

Osetljive kategorije podataka

Brunet protiv Francuske, br. 21010/10, 18. septembra 2014.

I. protiv Finske, br. 20511/03, 17. jula 2008.

Michaud protiv Francuske, br. 12323/11, 6. decembra 2012.

S. i Marper protiv Ujedinjenog Kraljevstva [VV], br. 30562/04 i 30566/04, 4. decembra 2008.

Nadzor i sprovođenje (uloga različitih subjekata, uključujući nadzorna tela)

I. protiv Finske, br. 20511/03, 17. jula 2008.

K. U. protiv Finske, br. 2872/02, 2. decembra 2008.

Von Hannover protiv Nemačke, br. 59320/00, 24. juna 2004.

Von Hannover protiv Nemačke (br. 2) [VV], br. 40660/08 i 60641/08, 7. februara 2012.

Metode nadzora

Allan protiv Ujedinjenog Kraljevstva, br. 48539/99, 5. novembra 2002.

Bărbulescu protiv Rumunije [VV], br. 61496/08, 5. septembra 2017.

D. L. protiv Bugarske, br. 7472/14, 19. maja 2016.

Dragojević protiv Hrvatske, br. 68955/11, 15. januara 2015.

Karabeyoğlu protiv Turske, br. 30083/10, 7. juna 2016.

Klass i drugi protiv Nemačke, br. 5029/71, 6. septembra 1978.

Roman Zakharov protiv Rusije [VV], br. 47143/06, 4. decembra 2015.

Rotaru protiv Rumunije [VV], br. 28341/95, 4. maja 2000.

Szabó i Vissy protiv Mađarske, br. 37138/14, 12. januara 2016.

Taylor-Sabori protiv Ujedinjenog Kraljevstva, br. 47114/99, 22. oktobra 2002.

Udruženje za europsku integraciju i ljudska prava i Ekimdzhiev protiv Bugarske, br. 62540/00, 28. juna 2007.

Uzun protiv Nemačke, br. 35623/05, 2. septembra 2010.

Versini-Campinchi i Crasnianski protiv Francuske, br. 49176/11, 16. juna 2016.

Vetter protiv Francuske, br. 59842/00, 31. maja 2005.

Vukota-Bojić protiv Švajcarske, br. 61838/10, 18. oktobra 2016.

Video-nadzor

Köpke protiv Nemačke, br. 420/07, 5. oktobra 2010.

Peck protiv Ujedinjenog Kraljevstva, br. 44647/98, 28. januara 2003.

Glasovni uzorci

P. G. i J. H. protiv Ujedinjenog Kraljevstva, br. 44787/98, 25. septembra 2001.

Wisse protiv Francuske, br. 71611/01, 20. decembra 2005.

Odabrana sudska praksa Suda pravde Evropske unije

Sudska praksa koja se odnosi na Direktivu o zaštiti podataka

C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde protiv Rīgas pašvaldības SIA „Rīgas satiksme”*, 4. maja 2017.

[Načelo zakonite obrade: zakonit interes treće strane]

C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce protiv Salvatorea Mannija*, 9. marta 2017.

[Pravo na brisanje ličnih podataka; pravo na prigovor na obradu]

Spojeni predmeti C-203/15 i C-698/15, *Tele2 Sverige AB protiv Post- och telestyrelsen i Secretary of State for the Home Department protiv Toma Watsona i drugih* [VV], 21. decembra 2016.

[Poverljivosti elektronskih komunikacija; pružaoci elektronskih komunikacionih usluga; obaveza koja se odnosi na opšte i neselektivno zadržavanje podataka o prometu i podataka o lokaciji; nepostojanje prethodnog nadzora suda ili nadzora nezavisnog upravnog tela; Povelja Evropske unije o osnovnim pravima; usklađenost s pravom Unije]

C-582/14, *Patrick Breyer protiv Bundesrepublik Deutschland*, 19. oktobra 2016.

[Pojam „lični podaci”; adrese internetskog protokola; čuvanje koje vrši pružalac usluga internet medija; nacionalni propis koji ne omogućava da rukovalac podacima uzme o obzir postavljeni zakoniti interes]

C-362/14, *Maximillian Schrems protiv Data Protection Commissioner* [VV], 6. oktobra 2015.

[Načelo zakonite obrade; osnovna prava; nevaženje Odluke o „sigurnoj luci”; ovlašćenja nacionalnih nadzornih tela]

C-230/14, *Weltimmo s. r. o. protiv Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1. oktobra 2015.

[Ovlašćenja nacionalnih nadzornih tela]

C-201/14, *Smaranda Bara i dr. protiv Casa Naţională de Asigurări de Sănătate i dr.*, 1. oktobra 2015.

[Pravo na obaveštavanje o obradi ličnih podataka]

C-212/13, *František Ryneš protiv Úřad pro ochranu osobních údajů*, 11. decembra 2014.

[Pojmovi „obrada podataka" i „rukovalac podacima"]

C-473/12, *Institut professionnel des agents immobiliers (IPI) protiv Geoffreyja Engleberta i dr.*, 7. novembra 2013.

[Pravo na obaveštavanje o obradi ličnih podataka]

T-462/12 R, *Pilkington Group Ltd protiv Evropske komisije*, Rešenje predsednika Opšteg suda, 11. marta 2013.

C-342/12, *Worten – Equipamentos para o Lar, SA protiv Autoridade para as Condições de Trabalho (ACT)*, 30. maja 2013.

[Pojam „lični podaci"; evidencija radnog vremena; načela povezana s kvalitetom podataka i kriterijumima za zakonitost obrade podataka; pristup nacionalnog tela nadležnog za nadzor radnih uslova; obaveza poslodavca da stavi na raspolaganje evidenciju o radnom vremenu radi neposrednog uvida]

Spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr. i Kärntner Landesregierung i dr.* [VV], 8. aprila 2014.

[Kršenje primarnog prava Unije Direktivom o zadržavanju podataka; zakonita obrada; ograničenje svrhe i čuvanja]

C-288/12, *Europska komisija protiv Mađarske* [VV], 8. aprila 2014.

[Zakonitost ukidanja kancelarije nacionalnog poverenika za zaštitu podataka]

Spojeni predmeti C-141/12 i C-372/12, *Y. S. protiv Minister voor Immigratie, Integratie en Asiel i Minister voor Immigratie, Integratie en Asiel protiv M. i S.*, 17. jula 2014.

[Opseg prava ispitanika na pristup; zaštita fizičkih lica u vezi s obradom ličnih podataka; pojam „ličnih podataka"; podaci koji se odnose na podnosioca zahteva za dozvolu za boravak i pravna analiza u pripremnom upravnom dokumentu za odluku; Povelja Evropske unije o osnovnim pravima]

C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje Gonzáleza* [VV], 13. maja 2014.

[Obaveze pružaoca internet pretraživača da na zahtev ispitanika ne prikazuju lične podatke u rezultatima pretrage; primenjivost Direktive o zaštiti podataka; pojam „obrada podataka"; značenje „rukovaoca podacima"; uspostavljanje ravnoteže između zaštite podataka i slobode izražavanja; pravo na zaborav]

C-614/10, *Evropska komisija protiv Republike Austrije* [VV], 16. oktobra 2012.

[Nezavisnost nacionalnog nadzornog tela]

Spojeni predmeti C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) protiv Administración del Estado*, 24. novembra 2011.

[Ispravno sprovođenje člana 7 tačke (f) Direktive o zaštiti podataka – „zakoniti interesi drugih" – u nacionalnom zakonodavstvu]

C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) protiv Netlog NV*, 16. februara 2012.

[Obaveza pružaoca usluga društvenih mreža u pogledu sprečavanja nezakonite upotrebe muzičkih i audio-vizuelnih radova od strane internet korisnika]

C-70/10, *Scarlet Extended SA protiv Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. novembra 2011.

[Informatička kompanija; autorsko pravo; internet; softver za povezivanje ravnopravnih računara; pružaoci internet usluga; instalacija sistema za filtriranje elektronskih komunikacija radi sprečavanja zajedničkog korišćenja datoteka kojim se krše autorska prava; nepostojanje opšte obaveze nadzora prenesenih informacija]

C-543/09, *Deutsche Telekom AG protiv Bundesrepublik Deutschland*, 5. maja 2011.

[Nužnost obnavljanja pristanka]

Spojeni predmeti C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen* [VV], 9. novembra 2010.

[Pojam „lični podaci"; proporcionalnost pravne obaveze objavljivanja ličnih podataka o korisnicima određenih subvencija iz poljoprivrednih fondova Evropske unije]

C-553/07, *College van burgemeester en wethouders van Rotterdam protiv M. E. E. Rijkeboer,* 7. maja 2009.

[Pravo ispitanika na pristup]

C-518/07, *Evropska komisija protiv Savezne Republike Nemačke* [VV], 9. marta 2010.

[Nezavisnost nacionalnog nadzornog tela]

C-73/07, *Tietosuojavaltuutettu protiv Satakunnan Markkinapörssi Oy i Satamedia Oy* [VV], 16. decembra 2008.

[Pojam „novinarskih delatnosti" u smislu člana 9 Direktive o zaštiti podataka]

C-524/06, *Heinz Huber protiv Bundesrepublik Deutschland* [VV], 16. decembra 2008.

[Zakonitost zadržavanja podataka o strancima u statističkom registru]

C-275/06, *Productores de Música de España (Promusicae) protiv Telefónica de España SAU* [VV], 29. januara 2008.

[Pojam „lični podaci"; obaveza pružaoca pristupa internetu da otkriju identitet korisnika programa za razmenu datoteka KaZaA udruženju za zaštitu intelektualne svojine]

C-101/01, *Krivični postupak protiv Bodil Lindqvist*, 6. novembra 2003.

[Posebne kategorije ličnih podataka]

Spojeni predmeti C-465/00, C-138/01 i C-139/01, *Rechnungshof protiv Österreichischer Rundfunk i dr. i Christa Neukomm i Joseph Lauermann protiv Österreichischer Rundfunk*, 20. maja 2003.

[Proporcionalnost pravne obaveze objave ličnih podataka o platama radnika određenih kategorija institucija povezanih s javnim sektorom]

C-434/16, *Peter Nowak protiv Data Protection Commissioner, Mišljenje nezavisne advokatice Kokott*, 20. jula 2017.

[Pojam ličnih podataka; pristup sopstvenom ispitnom radu; napomene ispravljača]

C-291/12, *Michael Schwarz protiv Stadt Bochum*, 17. oktobra 2013.

[Zahtev za prethodnu odluku; oblast slobode, bezbednosti i pravde; biometrijski pasoš; otisci prstiju; pravna osnova; srazmernost]

Sudska praksa koja se odnosi na Direktivu 2016/681

Mišljenje 1/15 Suda (veliko Veće), 26. jula 2017.

[Pravna osnova; Predlog sporazuma između Kanade i Evropske unije o prenosu i obradi podataka iz popisa imena vazduhoplovnih putnika; usklađenost Predloga sporazuma s članom 16 UFEU-a i članovima 7 i 8 i članom 52 stavom 1 Povelje Evropske unije o osnovnim pravima]

Sudska praksa koja se odnosi na Uredbu o zaštiti podataka u institucijama Evropske unije

C-615/13 P, *ClientEarth i Pesticide Action Network Europe (PAN Europe) protiv Evropske agencije za sigurnost hrane (EFSA) i Evropske komisije*, 16. jula 2015.

[Pristup dokumentima]

C-28/08 P, *Evropska komisija protiv The Bavarian Lager Co. Ltd* [VV], 29. juna 2010.

[Pristup dokumentima]

Sudska praksa koja se odnosi na Direktivu 2002/58/EZ

C-536/15, *Tele2 (Netherlands) BV i dr. protiv Autoriteit Consument en Markt (ACM)*, 15. marta 2017.

[Načelo nediskriminacije; stavljanje na raspolaganje ličnih podataka pretplatnika u svrhu njihove objave u telefonskom imeniku odnosno njihovo korišćenje u svrhu javno dostupne usluge davanja obaveštenja o brojevima pretplatnika; pretplatnikov pristanak; razlika u zavisnosti od države članice u kojoj se pruža javno dostupna usluga davanja obaveštenja o brojevima pretplatnika i/ili telefonskih imenika]

Spojeni predmeti C-203/15 i C-698/15, *Tele2 Sverige AB protiv Post- och telestyrelsen i Secretary of State for the Home Department protiv Toma Watsona i drugih* [VV], 21. decembra 2016.

[Poverljivosti elektronskih komunikacija; pružaoci elektronskih komunikacionih usluga; obaveza koja se odnosi na opšte i neselektivno zadržavanje podataka o prometu i podataka o lokaciji; nepostojanje prethodnog nadzora suda ili nadzora nezavisnog upravnog tela; Povelja Evropske unije o osnovnim pravima; usklađenost s pravom Unije]

C-70/10, *Scarlet Extended SA protiv Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. novembra 2011.

[Informatička kompanija; autorsko pravo; internet; softver za povezivanje ravnopravnih računara; pružaoci internet usluga; instalacija sistema za filtriranje elektronskih komunikacija radi sprečavanja zajedničkog korišćenja datoteka kojim se krše autorska prava; nepostojanje opšte obaveze nadzora prenesenih informacija]

C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB protiv Perfect Communication Sweden AB*, 19. aprila 2012.

[Autorsko pravo i srodna prava; obrada podataka putem interneta; kršenje isključivog prava; stavljanje audio-knjiga na raspolaganje putem FTP servera na internetu s IP adrese koju dodeljuje pružalac internet usluga; sudski nalog izdat pružaocu internet usluga kojim se zahteva da pruži ime i adresu korisnika IP adrese]

Index

Sudska praksa Suda pravde Evropske unije

Sudska praksa Evropskog suda za ljudska prava

Sudska praksa domaćih sudova

Mnoštvo informacija o Agenciji Evropske unije za osnovna prava dostupno je na internetu. Može im se pristupiti putem internet stranica FRA-a na fra.europa.eu.

Dodatne informacije o sudskoj praksi Evropskog suda za ljudska prava dostupne su na web-mestu Suda: echr.coe.int. Portal za pretraživanje HUDOC pruža pristup presudama i odlukama na engleskom i/ili francuskom jeziku, prevode na druge jezike, pravne sažetke, saopštenja za medije i druge informacije o radu Suda (http://hudoc.echr.coe.int).

Kako doći do izdanja Saveta Evrope

Council of Europe Publishing štampa deluje u svim područjima rada organizacije, uključujući ljudska prava, pravne nauke, zdravstvo, etičnost, društvena pitanja, životnu sredinu, obrazovanje, kulturu, sport, mlade i arhitektonsko nasleđe. Knjige i elektronske publikacije iz opsežnog kataloga mogu se naručiti putem interneta (http://book.coe.int/).

Virtuelna čitaonica korisnicima omogućava da besplatno prouče isečke iz glavnih radova koji su upravo objavljeni ili celovite tekstove određenih službenih dokumenata.

Informacije o konvencijama Saveta Evrope i njihovi celoviti tekstovi dostupni su putem veb sajta Kancelarije za ugovore: http://conventions.coe.int/.

doi: 10.2811/343461 TK-05-17-225-EN-N

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Brz razvoj informacione tehnologije povećao je potrebu za snažnom zaštitom ličnih podataka. To pravo je zaštićeno instrumentima i Evropske unije (EU) i Saveta Evrope (SE). Zaštita tog važnog prava podrazumeva nove i značajne izazove, dok tehnološki napredak prouzrokuje pomeranje granica oblasti kao što su nadzor, presretanja komunikacija i čuvanje podataka. Ovaj priručnik je namenjen pravnicima koji nisu specijalizirali u oblasti zaštite podataka kako bi se upoznali s ovom novom oblašću prava. Priručnik sadrži pregled primenjivih pravnih okvira Evropske unije i Saveta Evrope. U njemu se takođe objašnjava ključna sudska praksa i sažimaju najvažnije presude Suda pravde Evropske unije i Evropskog suda za ljudska prava. Usto, u priručniku su predstavljeni hipotetički scenariji koji služe kao praktične ilustracije različitih problema koji se javljaju u ovoj oblasti koja se neprekidno razvija.

FRA – AGENCIJA EVROPSKE UNIJE ZA OSNOVNA PRAVA
Schwarzenbergplatz 11 – 1040 Beč – Austrija
Tel. +43 158030-0 – Faks +43 158030-699
fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

EVROPSKI SUD ZA LJUDSKA PRAVA
SAVET EVROPE
67075 Strasbourg Cedex – Francuska
Tel.: +33 (0) 3 88 41 20 18 – Fax +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int

EVROPSKI NADZORNIK ZA ZAŠTITU PODATAKA
Rue Wiertz 60 – 1047 Bruxelles – Belgija
Tel.: +32 2 283 19 00
www.edps.europa.eu – edps@edps.europa.eu – @EU_EDPS