PRIRUČNIK

Priručnik o europskom zakonodavstvu o zaštiti podataka

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

Rukopis ovoga priručnika završen je u prosincu 2014.
Ažurirane verzije ubuduće će biti na raspolaganju na internetskoj stranici Agencije Europske unije za temeljna prava (FRA) na adresi: fra.europa.eu, na internetskoj stranici Vijeća Europe: coe.int/dataprotection, te na internetskoj stranici Europskog suda za ljudska prava u izborniku Sudska praksa na adresi: echr.coe.int.

Europe Direct je usluga koja Vam pomaže u pronalasku odgovora na Vaša pitanja o Europskoj uniji.

Besplatni broj telefona (*):

00 800 6 7 8 9 10 11

(*) Dana informacija je besplatna, kao i većina poziva (neki operateri, phone box-ovi ili hoteli mogu Vam naplatiti).

Fotografija (naslovnica i unutrašnjost): © iStockphoto

Više informacija o Europskoj uniji pronađite na Internetu (http://europa.eu).

Podaci o kategorizaciji mogu se pronaći pri kraju ove publikacije.

Luksemburg: Ured za publikacije Europske unije, 2014.

ISBN 978-92-871-9945-4 (CoE)
ISBN 978-92-9239-333-5 (FRA)
doi:10.2811/53863

Printed in Belgium

Tiskano na recikliranom papiru u postupku bez korištenja klora (PCF)

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

Priručnik o europskom zakonodavstvu o zaštiti podataka

Predgovor

Ovaj su priručnik o europskom zakonodavstvu o zaštiti podataka zajednički izradili Agencija Europske unije za temeljna prava (FRA) i Vijeće Europe u suradnji s tajništvom Europskog suda za ljudska prava. To je treći pravni priručnik u nizu koji su zajednički izradili FRA i Vijeće Europe. Prvi priručnik o europskom antidiskriminacijskom pravu objavljen je u ožujku 2011. dok je u lipnju 2013. objavljen i sljedeći priručnik o europskom pravu vezanom uz azil, granice i imigraciju.

Odlučili smo nastaviti dosadašnju suradnju i prihvatiti se vrlo aktualne teme s kojom se svakodnevno susrećemo, odnosno zaštite osobnih podataka. Europa ima jedan od najboljih sustava zaštite u ovome području koji se zasniva na Konvenciji br. 108 Vijeća Europe, pravnim aktima Europske unije (EU) te sudskoj praksi Europskog suda za ljudska prava i Suda Europske unije.

Cilj je ovoga priručnika doprinijeti boljoj informiranosti o propisima o zaštiti podataka u državama članicama Europske unije i Vijeća Europe služeći čitateljima kao glavna referentna točka. Namijenjen je nespecijaliziranim pravnicima, sucima, nacionalnim tijelima nadležnim za zaštitu podataka i drugim osobama koje se bave zaštitom podataka.

Stupanjem na snagu Ugovora iz Lisabona u prosincu 2009., Povelja EU-a o temeljnim pravima postala je pravno obvezujuća te je pravo na zaštitu osobnih podataka dobilo status zasebnog temeljnog prava. Za zaštitu ovoga temeljnog prava od ključnog je značaja bolje razumijevanje Konvencije br. 108 Vijeća Europe i akata EU-a koji su utrli put zaštiti podataka u Europi, kao i sudske prakse ECtHR i CJEU.

Želimo zahvaliti Institutu za ljudska prava Ludwig Botzmann za njegovo sudjelovanje u pripremanju ovog priručnika. Također želimo zahvaliti Uredu Europskog nadzornika za zaštitu podataka za pruženu pomoć tijekom izrade priručnika. Posebno zahvaljujemo jedinici za zaštitu podataka Europske komisije na njezinu pomoć. Konačno želimo zahvaliti hrvatskoj Agenciji za zaštitu osobnih podataka, na pregledu hrvatskog prijevoda ovog Priručnika.

Philippe Boillat

Glavni direktor
Odjela za ljudska prava i vladavinu prava
Vijeće Europe

Morten Kjaerum

Direktor
Agencije Europske unije
za temeljna prava

Sadržaj

Kratice i akronimi

BCR	Obvezujuće pravilo poduzeća
CCTV	Televizija zatvorenog kruga
CETS	Zbirka ugovora Vijeća Europe
Povelja	Povelja Europske unije o temeljnim pravima
CIS	Carinski informacijski sustav
CJEU	Sud Europske unije (prije prosinca 2009. poznat kao Europski sud, ECJ)
CoE	Vijeće Europe
Konvencija br. 108	Konvencija o zaštiti pojedinaca pri automatskoj obradi osobnih podataka (Vijeće Europe)
CRM	Upravljanje odnosima s kupcima
C-SIS	Središnji schengenski informacijski sustav
EAW	Europski uhidbeni nalog
EC	Europska zajednica (EZ)
ECHR	Europska konvencija o ljudskim pravima
ECtHR	Europski sud za ljudska prava
EDPS	Europski nadzornik za zaštitu podataka
EGP	Europski gospodarski prostor
EFTA	Europska udruga slobodne trgovine
ENISA	Europska agencija za mrežnu i informacijsku sigurnost
ENU	Europolova nacionalna jedinica
ESMA	Europsko nadzorno tijelo za vrijednosne papire i tržišta kapitala
eTEN	Transeuropske telekomunikacijske mreže
EU	Europska unija
EuroPriSe	Europski pečat za zaštitu podataka

eu-LISA	Agencija Europske unije za operativno upravljanje velikim informatičkim sustavima
FRA	Agencija Europske unije za temeljna prava
GPS	Globalni sustav pozicioniranja
JSB	Zajedničko nadzorno tijelo
NGO	Nevladina organizacija
N-SIS	Nacionalni schengenski informacijski sustav
OECD	Organizacija za gospodarsku suradnju i razvoj
PIN	Osobni identifikacijski broj
PNR	Evidencija imena putnika
SEPA	Jedinstveno područje plaćanja u eurima
SIS	Schengenski informacijski sustav
SWIFT	Društvo za svjetsku međubankovnu financijsku telekomunikaciju
TEU	Ugovor o Europskoj uniji
TFEU	Ugovor o funkcioniranju Europske unije
UDHR	Opća deklaracija o ljudskim pravima
UN	Ujedinjeni narodi
VIS	Vizni informacijski sustav

Kako koristiti priručnik

Ovaj priručnik daje uvid u zakonodavstvo primjenjivo na zaštitu podataka koje se odnosi na Europsku uniju (EU) i Vijeće Europe (CoE).

Priručnik je osmišljen kao pomoć pravnicima koji nisu specijalizirani u području zaštite podataka; namijenjen je odvjetnicima, sucima i drugim pravnim djelatnicima kao i zaposlenicima drugih tijela, uključujući nevladine organizacije (NGO) koji se mogu susresti s pravnim pitanjima vezanim uz zaštitu podataka.

On je prva referentna točka o pravu Europske unije i Europskoj konvenciji o ljudskim pravima (ECHR) kada je u pitanju zaštita podataka. Objašnjava kako je to područje regulirano unutar prava Europske unije i Konvencije o ljudskim pravima kao i Konvencije Vijeća Europe o zaštiti pojedinaca pri automatskoj obradi osobnih podataka (Konvencija br. 108) i drugih akata Vijeća Europe. U svakom je poglavlju uvodno prikazana tablica s primjenjivim propisima uključujući izbor važnih sudskih praksi iz dva zasebna europska pravna sustava. Zatim su relevantni zakoni tih dvaju europskih sustava predstavljeni jedan po jedan prema primjenjivosti na svaku od tema. To čitatelju omogućuje uvid u sličnosti i razlike dvaju pravnih sustava.

U uvodnim tablicama svakoga poglavlja navedene su teme kojima se određeno poglavlje bavi kao i primjenjivi propisi i ostali bitan materijal, kao što je sudska praksa. Redoslijed tema može se ponešto razlikovati od strukture teksta poglavlja ako to ide u prilog konciznom predstavljanju sadržaja poglavlja. Tablice uključuju i pravo Vijeća Europe i pravo Europske unije. To bi čitateljima trebalo pomoći u pronalaženju ključnih informacija koje se tiču njihova slučaja, osobito ako podliježu samo pravu Vijeća Europe.

Pravnici u državama koje nisu članice Unije, ali su članice Vijeća Europe te stranke Europske konvencije o ljudskim pravima i Konvencije br. 108, mogu pogledati informacije koje se tiču njihove države izravno u odjeljcima koji se odnose na Vijeće Europe. Pravnici u državama članicama Unije moraju pogledati oba odjeljka jer su za te države obvezujuća oba pravna poretka. Za sve koji trebaju podrobnije informacije o određenoj temi, predviđen je odjeljak priručnika pod nazivom „Dodatna literatura".

Pravo Vijeća Europe predstavljeno je kroz kratka upućivanja na odabrane slučajeve Europskog suda za ljudska prava (ECtHR). Oni su odabrani iz velikog broja presuda i odluka ovoga suda u slučajevima koji se tiču zaštite podataka.

Pravo Europske unije nalazi se u usvojenim zakonodavnim mjerama, mjerodavnim odredbama ugovora te u Povelji Europske unije o temeljnim pravima, prema tumačenjima sudske prakse Suda Europske unije (CJEU, koji je prije prosinca 2009. bio poznat kao Europski sud (ECJ)).

Sudska praksa koja je opisana ili citirana u ovome priručniku daje primjere važnog korpusa sudskih praksi Europskog suda za ljudska prava i Suda Europske unije. Smjernice na kraju priručnika služe kao pomoć čitatelju u traženju sudske prakse na internetu.

Nadalje, praktične ilustracije s hipotetskim scenarijima u tekstualnim okvirima služe kao dodatno objašnjenje primjene europskih pravila o zaštiti podataka u praksi, osobito u slučajevima nepostojanja konkretne sudske prakse Europskog suda za ljudska prava ili Suda Europske unije.

U uvodnom dijelu priručnika ukratko je opisana uloga dvaju pravnih sustava koja su uspostavljena Europskom konvencijom o ljudskim pravima i pravom Unije (poglavlje 1.). Poglavlja od 2. do 8. obuhvaćaju sljedeće teme:

- terminologija vezana uz zaštitu podataka
- glavna načela europskog zakonodavstva o zaštiti podataka
- propisi europskog zakonodavstva o zaštiti podataka
- prava osoba čiji se podaci obrađuju i njihova provedba
- prekogranični prijenos podataka
- zaštita podataka u kontekstu policije i kaznenog pravosuđa
- drugo specifično europsko zakonodavstvo o zaštiti podataka.

1

Kontekst i pozadina europskog zakonodavstva o zaštiti podataka

EU	Pitanja kojima se bavi	Vijeće Europe
Pravo na zaštitu podataka		
Direktiva 95/46/EZ o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (*Direktiva o zaštiti podataka*), SL L 1995 L 281.		Europska konvencija o ljudskim pravima (ECHR), članak 8. (pravo na poštovanje privatnog i obiteljskog života, doma i dopisivanja) Konvencija o zaštiti pojedinaca pri automatskoj obradi osobnih podataka (Konvencija br. 108)
Uravnoteživanje prava		
CJEU, zajednički slučajevi C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen*, 2010.	**Općenito**	
CJEU, C-73/07, *Tietosuojavaltuutettu protiv Satakunnan Markkinapörssi Oy i Satamedia Oy*, 2008.	**Sloboda izražavanja**	ECtHR, *Axel Springer AG protiv Njemačke*, 2012. ECtHR, *Mosley protiv Ujedinjene Kraljevine*, 2011.
	Sloboda umjetnosti i znanosti	ECtHR, *Vereinigung bildender Künstler protiv Austrije*, 2007.
CJEU, C-275/06, *Productores de Música de España (Promusicae) protiv Telefónica de España SAU*, 2008.	**Zaštita vlasništva**	
CJEU, C-28/08 P, *Europska komisija protiv The Bavarian Lager Co. Ltd*, 2010.	**Pristup dokumentima**	ECtHR, *Társaság a Szabadságjogokért protiv Mađarske*, 2009.

1.1. Pravo na zaštitu podataka

Ključne točke

- Prema članku 8. Europske konvencije o ljudskim pravima, pravo na zaštitu od prikupljanja i uporabe osobnih podataka dio je prava na poštovanje privatnog i obiteljskog života, doma i dopisivanja.
- Konvencija br. 108 Vijeća Europe prvi je međunarodni obvezujući akt koji se izričito bavi zaštitom podataka.
- Unutar prava Europske unije, zaštita podataka prvi je put regulirana Direktivom o zaštiti podataka.
- Unutar prava Europske unije, zaštita podataka priznata kao temeljno pravo.

Pravo na zaštitu privatnog života pojedinca od drugih, a osobito države, prvi je put propisano međunarodnim pravnim aktom u članku 12. Opće deklaracije o ljudskim pravima (UDHR) Ujedinjenih naroda (UN) iz 1948. o poštovanju privatnog i obiteljskog života.[1] Opća deklaracija o ljudskim pravima utjecala je na razvoj drugih akata o ljudskim pravima u Europi.

1.1.1. Europska konvencija o ljudskim pravima

Vijeće Europe osnovano je nakon Drugog svjetskog rata kako bi približilo države Europe u nastojanjima za promicanjem vladavine prava, demokracije, ljudskih prava i društvenog razvoja. U tu je svrhu Vijeće 1950. usvojilo Europsku konvenciju o ljudskim pravima (ECHR) koja je stupila na snagu 1953.

Države imaju međunarodnu obvezu poštivanja Konvencije. Sve članice Vijeća Europe ugradile su ili provele Konvenciju u svojim nacionalnim zakonodavstvima, što ih obvezuje na poštivanje odredbi Konvencije.

Kako bi se osiguralo da ugovorne stranke poštuju svoje obveze preuzete Konvencijom, u francuskom je Strasbourgu 1959. osnovan Europski sud za ljudska prava (ECtHR). Taj sud osigurava da države poštuju obveze preuzete Konvencijom razmatrajući žalbe pojedinaca, skupina pojedinaca, nevladinih organizacija ili pravnih osoba zbog navodnog kršenja Konvencije. Vijeće Europe je 2013. brojilo 47 država članica od kojih su 28 i države članice Europske unije. Podnositelj koji se obraća Europskom

1 Ujedinjeni narodi (UN), Opća deklaracija o ljudskim pravima (UDHR), 10. prosinca 1948.

sudu za ljudska prava ne mora biti državljanin članice Europske unije. Taj sud može razmatrati i međudržavne zahtjeve koje je jedna država članica Vijeća Europe (ili više njih) podnijela protiv druge države članice.

Pravo na zaštitu osobnih podataka dio je prava zaštićenih člankom 8. Konvencije kojim se jamči pravo na poštovanje privatnog i obiteljskog života, doma i dopisivanja te propisuju uvjeti u kojima su dopuštena ograničenja toga prava.[2]

Europski sud za ljudska prava u svojoj je sudskoj praksi imao priliku razmotriti mnoge situacije koje su se ticale pitanja zaštite podataka, primjerice presretanje komunikacije,[3] razne oblike nadzora[4] i zaštitu od pohrane osobnih podataka od strane javnih tijela.[5] Pojasnio je da članak 8. Konvencije ne samo da obvezuje države na suzdržavanje od svih radnji kojima bi mogle prekršiti to pravo iz Konvencije, već i da ih u određenim okolnostima pozitivno obvezuje na aktivno promicanje učinkovitog poštivanja privatnog i obiteljskog života.[6] Mnogi će se od tih slučajeva detaljno razmotriti u odgovarajućim poglavljima.

1.1.2. Konvencija br. 108 Vijeća Europe

Od pojave informacijske tehnologije 60-ih godina prošloga stoljeća, rasla je potreba za detaljnijim propisima kojima bi se zaštitili (osobni) podaci pojedinaca. Sredinom 70-ih godina Odbor ministara Vijeća Europe usvojio je više rezolucija o zaštiti osobnih podataka pozivajući se na članak 8. Europske konvencije o ljudskim pravima.[7] Godine 1981. za potpisivanje je otvorena Konvencija Vijeća Europe o zaštiti pojedinaca pri automatskoj obradi osobnih podataka (Konvencija br. 108).[8] Konvencija

2 CoE, Europska konvencija o ljudskim pravima, CETS br. 005, 1950.

3 Vidjeti primjerice ECtHR, *Malone protiv Ujedinjene Kraljevine*, br. 8691/79, 2. kolovoza 1984.; ECtHR, *Copland protiv Ujedinjene Kraljevine,* br. 62617/00, 3. travnja 2007.

4 Vidjeti primjerice ECtHR, *Klass i drugi protiv Njemačke*, br. 5029/71, 6. rujna 1978.; ECtHR, *Uzun protiv Njemačke*, br. 35623/05, 2. rujna 2010.

5 Vidjeti primjerice ECtHR, *Leander protiv Švedske*, br. 9248/81, 26. ožujka 1987.; ECtHR, *S. i Marper protiv Ujedinjene Kraljevine*, br. , 30562/04 i 30566/04, 4. prosinca 2008.

6 Vidjeti primjerice ECtHR, *I. protiv Finske*, br. 20511/03, 17. srpnja 2008.; ECtHR, *K.U. protiv Finske*, br. 2872/02, 2. prosinca 2008.

7 CoE, Odbor ministara (1973), Rezolucija (73) 22 o zaštiti privatnosti pojedinaca *vis-à-vis* elektroničkih banki podataka u privatnom sektoru, 26. rujna 1973.; CoE, Odbor ministara (1974.), Rezolucija (74) 29 o zaštiti privatnosti pojedinaca *vis-à-vis* elektroničkih banki podataka u javnom sektoru, 20. rujna 1974.

8 CoE, Konvencija o zaštiti pojedinaca pri automatskoj obradi osobnih podataka, Vijeće Europe, CETS br. 108, 1981.

br. 108 bila je i ostala jedini pravno obvezujući međunarodni akt u području zaštite podataka.

Konvencija br. 108 se primjenjuje na obradu osobnih podataka u privatnom i u javnom sektoru, kao na primjer u sudstvu i kod tijela nadležnih za osiguranje primjene zakona. Konvencija štiti pojedinca od zloporaba prilikom prikupljanja i obrade osobnih podataka nastojeći istodobno regulirati prekogranični prijenos osobnih podataka. U pogledu prikupljanja i obrade osobnih podataka, načela iz Konvencije osobito se tiču pravednog i zakonitog prikupljanja i automatske obrade podataka pohranjenih u određene legitimne svrhe, koji nisu namijenjeni uporabi neprimjerenoj takvim svrhama, i koji se ne smiju zadržavati dulje no što je to potrebno. Ta se načela tiču i kvalitete podataka. Oni u prvom redu moraju biti prikladni, relevantni, točni i ne pretjerani (razmjernost).

Osim jamstva u pogledu prikupljanja i obrade osobnih podataka, Konvencija, u odsutnosti prikladnih pravnih mjera zaštite, brani obradu „osjetljivih" podataka, kao što su rasa, političko opredjeljenje, zdravlje, vjera, seksualni život ili kaznena evidencija pojedinca.

Ona također štiti pravo pojedinca na informiranost o tome pohranjuju li se o njemu podaci, te, ako je to nužno, ispravljanje takvih podataka. Ograničenja u pogledu prava iz Konvencije moguća su samo kada su posrijedi prevladavajući interesi, kao što su državna sigurnost ili obrana.

Iako Konvencija omogućuje slobodan prijenos osobnih podataka među državama strankama Konvencije, ona također nameće određena ograničenja u pogledu takvih prijenosa u države čije pravno uređenje ne pruža jednaku razinu zaštite.

Kako bi nastavilo razvijati opća načela i pravila iz Konvencije br. 108, Odbor ministara Vijeća Europe usvojio je nekoliko pravno neobvezujućih preporuka (vidjeti poglavlja 7. i 8.).

Sve su članice Unije ratificirale Konvenciju br. 108. Ona je izmijenjena 1999. kako bi se Europskoj uniji omogućilo da postane stranka.[9] Dodatni protokol uz Konvenciju br. 108 usvojen je 2001. uvodeći odredbe o prekograničnom prijenosu podataka

9 CoE, Izmjene Konvencije o zaštiti pojedinaca pri automatskoj obradi osobnih podataka (ETS br. 108) kojima je omogućen pristup Europskim zajednicama, koje je Odbor ministara usvojio u Strasbourgu, 15. lipnja 1999.; čl. 23. stavak 2. Konvencije br. 108 u izmijenjenom obliku.

nečlanicama, tzv. trećim zemljama, te o obveznom uspostavljanju nacionalnih tijela nadležnih za zaštitu podataka.[10]

Izgledi

Nakon odluke o modernizaciji Konvencije br. 108 javno savjetovanje provedeno u 2011. omogućilo je potvrdu dvaju glavnih ciljeva toga zahvata: veća zaštita privatnosti u digitalno doba i jačanje mehanizma praćenja Konvencije.

Konvenciji br. 108 mogu pristupiti države koje nisu članice Vijeća Europe, uključujući i neeuropske zemlje. Potencijal Konvencije kao univerzalnog standarda i njen otvoren karakter mogu poslužiti kao temelj promicanja zaštite podataka na globalnoj razini.

Do sada su 45 od 46 ugovornih stranaka Konvencije br. 108 države članice Vijeća Europe. Urugvaj, prva neeuropska zemlja, Konvenciji je pristupio u kolovozu 2013., a Maroko, koji je Odbor ministara pozvao da pristupi Konvenciji br. 108, je u postupku formaliziranja pristupa.

1.1.3. Zakonodavstvo Europske unije o zaštiti podataka

Pravo Europske unije sastoji se od ugovora i sekundarnog prava Unije. Ugovore, odnosno Ugovor o Europskoj uniji (TEU) i Ugovor o funkcioniranju Europske unije (TFEU), odobrile su sve države članice EU-a, a nazivaju se još „primarno pravo Europske unije". Uredbe, direktive i odluke Europske unije donijele su njezine institucije koje su za to ovlaštene ugovorima; ti se akti često nazivaju „sekundarno pravo Europske unije".

Temeljni pravni akt o zaštiti podataka Europske unije je Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (*Direktiva o zaštiti podataka*).[11] Donesena je 1995., kada je nekoliko država članica već usvojilo nacionalne zakone o zaštiti podataka. Preduvjet za slobodno kretanje robe, kapitala, usluga i ljudi na unutarnjem tržištu bio je slobodan prijenos podataka koji se nije mogao

10 CoE, Dodatni protokol uz Konvenciju o zaštiti pojedinaca pri automatskoj obradi osobnih podataka, koji se tiče nadzornih tijela i prekograničnih prijenosa podataka, CETS br. 181, 2001.

11 Direktiva o zaštiti podataka, SL L 1995 L 281, str. 31.

ostvariti bez pouzdane i ujednačeno visoke razine zaštite podataka u državama članicama.

Budući da je cilj Direktive o zaštiti podataka bio uskladiti[12] zakonodavstva o zaštiti podataka na nacionalnoj razini, direktivi je svojstvena doza specifičnosti usporediva s tadašnjim nacionalnim zakonodavstvima o zaštiti podataka. Za CJEU, „Direktiva 95/46 je namijenjena [...] osiguranju jednake razine zaštite prava i sloboda pojedinaca u svakoj državi članici, u svezi s obradom osobnih podataka. [...] Ujednačavanje razine zaštite koju pružaju nacionalna zakonodavstva ne smije biti posljedica smanjivanja pružene razine zaštite, već upravo suprotno, mora se težiti osiguranju visoke razine zaštite u cijeloj Europskoj uniji. U skladu s time, usklađivanje nacionalnih zakonodavstava nije ograničeno na najnižu razinu ujednačavanja, već je cilj postizanje općeg usklađivanja".[13] Slijedom navedenog, države članice imaju tek ograničen manevarski prostor u provedbi direktive.

Direktiva o zaštiti podataka osmišljena je kako bi potvrdila i proširila načela prava na privatnost koja su već sadržana u Konvenciji br. 108. Činjenica da su sve od 15 država članica Europske unije 1995. bile i ugovorne stranke Konvencije br. 108 otklanjala je mogućnost usvajanja proturječnih propisa u ova dva pravna instrumenta. Ipak, u Direktivi o zaštiti podataka ostavljena je mogućnost dodavanja instrumenata zaštite, osigurana člankom 11. Konvencije br. 108. Uvođenje neovisnog nadzora kao instrumenta za bolju usklađenost s propisima o zaštiti podataka pokazalo se važnim doprinosom učinkovitom funkcioniraju europskog zakonodavstva o zaštiti podataka. (Taj je instrument 2001. preuzet u pravu Vijeća Europe Dodatnim protokolom uz Konvenciju br. 108.)

Teritorijalna primjenjivost Direktive o zaštiti podataka prelazi granice 28 država članica Unije i uključuje države koje nisu njene članice, ali su dio Europskog gospodarskog prostora (EGP)[14] – odnosno Island, Lihtenštajn i Norvešku.

CJEU sa sjedištem u Luksemburgu nadležan je odlučivati o tome je li određena država članica ispunila svoje obveze iz Direktive o zaštiti podataka kao i za prethodno odlučivanje o valjanosti i tumačenju direktive kako bi se osigurala njena učinkovita i jednaka primjena u državama članicama. Važno izuzeće od primjenjivosti Direktive o

12 Vidjeti primjerice Direktivu o zaštiti podataka, uvodne izjave 1., 4., 7. i 8.

13 CJEU, zajednički slučajevi 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. studenog 2011., odlomci 28-29.

14 Sporazum o Europskom gospodarskom prostoru, SL L 1994 L 1, na snazi od 1. siječnja 1994.

zaštiti podataka predstavlja takozvano izuzeće kućanstva, odnosno obrada osobnih podataka od strane fizičkih osoba u osobne svrhe ili u svrhe kućanstva.[15] Takva se obrada općenito smatra dijelom sloboda pojedinaca.

Sukladno primarnom pravu Europske unije koje je bilo na snazi u vrijeme usvajanja Direktive o zaštiti podataka, važno područje primjene direktive ograničeno je na pitanja unutarnjeg tržišta. Izvan područja primjene su pitanja suradnje policije i kaznenog pravosuđa. Zaštita podataka u ovim područjima proizlazi iz različitih pravnih akata koji su detaljnije opisani u poglavlju 7.

Budući da je Direktiva o zaštiti podataka mogla biti upućena samo državama članicama Unije, valjalo je uvesti dodatni pravni akt kako bi se osigurala zaštita podataka pri obradi osobnih podataka u institucijama i tijelima Europske unije. To je učinjeno Uredbom (EZ) br. 45/2001 o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka (*Uredba o zaštiti podataka u institucijama Europske unije*).[16]

Nadalje, čak su i u područjima koja su obuhvaćena u Direktivi o zaštiti podataka često potrebne detaljnije odredbe o zaštiti podataka kako bi se postigla nužna jasnoća kod uravnoteživanja drugih legitimnih interesa. Dva su primjera za to Direktiva 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (*Direktiva o privatnosti i elektroničkim komunikacijama*)[17] i Direktiva 2006/24/EZ o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža i o izmjeni Direktive 2002/58/EZ (*Direktiva o zadržavanju podataka*, proglašena nevaljanom 8. travnja 2014.).[18] O ostalim će se primjerima raspravljati u poglavlju 8. Takve odredbe moraju biti u skladu s Direktivom o zaštiti podataka.

15 Direktiva o zaštiti podataka, čl. 3. st. 2. druga alineja.

16 Uredba (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka SL L 2001 L 8.

17 Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (*Direktiva o privatnosti i elektroničkim komunikacijama*), SL L 2002 L 201.

18 Direktiva 2006/24/EZ Europskog parlamenta i Vijeća od 15. ožujka 2006. o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža i o izmjeni Direktive 2002/58/EZ (*Direktiva o zadržavanju podataka,* proglašena nevaljanom 8. travnja 2014.)*,* SL L 2006 L 105.

Povelja Europske unije o temeljnim pravima

Izvorni ugovori Europskih zajednica nisu se uopće bavili ljudskim pravima ili njihovom zaštitom. No na adresu tadašnjeg Europskog suda (ECJ) počeli su pristizati slučajevi o navodnoj povredi ljudskih prava u područjima unutar područja primjene prava Europske unije pa je sud razvio novi pristup toj problematici. Kako bi zajamčio zaštitu pojedincima, ugradio je temeljna prava u takozvana opća načela europskog prava. Prema Sudu Europske unije, ta opća načela odražavaju sadržaj zaštite ljudskih prava iz nacionalnih ustava i ugovora o ljudskim pravima, a osobito Konvencije o ljudskim pravima. Sud je smatrao da će osigurati sukladnost prava Europske unije s tim načelima.

Uviđajući da njene politike mogu utjecati na ljudska prava i nastojeći izgraditi „bliskiji" odnos sa svojim državljanima, Europska unija je 2000. proglasila Povelju Europske unije o temeljnim pravima (Povelja). Ona obuhvaća čitav spektar civilnih, političkih, ekonomskih i socijalnih prava europskih građana i sintetizira ustavne tradicije i međunarodne obveze zajedničke državama članicama. Prava opisana u Povelji dijele se u šest kategorija: dostojanstvo, slobode, jednakost, solidarnost, prava građana i pravda.

Iako je Povelja isprva bila samo politički dokument, stupanjem na snagu Ugovora iz Lisabona 1. prosinca 2009., postala je pravno obvezujuća[19] kao primarno pravo Europske unije (vidjeti članak 6. stavak 1. Ugovora o Europskoj uniji).[20]

Primarno pravo Europske unije sadrži i opću sposobnost Unije za donošenje zakona koji se tiču zaštite podataka (članak 16. Ugovora o funkcioniranju Europske unije).

Povelja ne jamči samo poštovanje privatnog i obiteljskog života (članak 7.), već i utvrđuje pravo na zaštitu podataka (članak 8.), jer se njome izričito podiže razina te vrste zaštite do one koju uživaju temeljna prava u pravu Europske unije. Institucije Europske unije baš kao i države članice moraju poštivati i jamčiti to pravo, što se primjenjuje i na države članice pri provedbi prava Unije (članak 51. Povelje). Formuliran nekoliko godina nakon Direktive o zaštiti podataka, članak 8. Povelje valja shvatiti na način da utjelovljuje postojeće zakonodavstvo o zaštiti podataka Europske unije. Stoga Povelja, osim što u članku 8. stavku 1. izričito spominje pravo na

19 EU (2012), Povelja Europske unije o temeljnim pravima, SL L 2012 C 326.

20 Vidjeti pročišćene verzije Europskih zajednica (2012.), Ugovor o Europskoj uniji, SL L 2012 C 326; i Europskih zajednica (2012.), Ugovor o funkcioniranju Europske unije, SL L 2012 C 326.

zaštitu podataka, upućuje i na ključna načela zaštite podataka u članku 8. stavku 2. I konačno, člankom 8. stavkom 3. Povelje osigurava se da će neovisno tijelo vršiti kontrolu provedbe tih načela.

Izgledi

U siječnju 2012. Europska komisija predložila je paket reformi zaštite podataka držeći da treba modernizirati trenutne propise o zaštiti podataka u svjetlu rastućeg tehnološkog napretka i globalizacije. Paket reformi sastoji se od prijedloga Opće uredbe o zaštiti podataka,[21] kojom bi se zamijenila Direktiva o zaštiti podataka, te od nove Direktive o zaštiti podataka[22] kojom će se osigurati zaštita podataka u područjima suradnje policije i kaznenog pravosuđa u kaznenim predmetima. U vrijeme objave ovoga priručnika još su se vodile rasprave o paketu reformi.

1.2. Uravnoteživanje prava

Ključne točke

- Pravo na zaštitu podataka nije apsolutno pravo; ono se mora uravnotežiti s drugim pravima.

Temeljno pravo na zaštitu osobnih podataka prema članku 8. Povelje „ipak nije apsolutno pravo, već ga treba promatrati s obzirom na njegovu funkciju u društvu."[23] Članak 52. stavak 1. Povelje tako prihvaća mogućnost nametanja ograničenja pri provedbi prava, poput onih iz članaka 7. i 8. Povelje, pod uvjetom da su takva ograničenja zakonita, da poštuju suštinu tih prava i sloboda te da su sukladno načelu razmjernosti nužna i da istinski ispunjavaju ciljeve od općeg interesa koje je prepoznala Europska unija, ili pak potrebu zaštite tuđih prava i sloboda.[24]

21 Europska komisija (2012), *Prijedlog Uredbe Europskog parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (Opća uredba o zaštiti podataka)*, COM(2012) 11 konačno, Bruxelles, 25. siječnja 2012.

22 Europska komisija (2012), *Prijedlog Uredbe Europskog parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka u ovlaštenim tijelima u svrhe sprečavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kazni te o slobodnom protoku takvih podataka (Opća direktiva o zaštiti podataka)*, COM(2012) 10 konačno, Bruxelles, 25. siječnja 2012.

23 Vidjeti primjerice CJEU, zajednički slučajevi C-92/09 i C-93/09, *Volker i Markus Schecke GbR i Hartmut Eifert protiv Land Hessen*, 9. studenoga 2010., st. 48.

24 *Ibid.*, st. 50.

U okviru Europske konvencije o ljudskim pravima zaštita podataka zajamčena je člankom 8. (pravo na poštovanje privatnog i obiteljskog života) pa se to pravo, analogno Povelji, mora primjenjivati poštujući područje primjene drugih konkurentskih prava. Sukladno članku 8. stavku 2. Konvencije „Javna vlast se neće miješati u ostvarivanje tog prava, osim u skladu sa zakonom i ako je u demokratskom društvu nužno [...] radi zaštite prava i sloboda drugih."

Shodno tome, i Europski sud za ljudska prava i Sud Europske unije višekratno su naglašavali da je u primjeni i tumačenju članka 8. Konvencije i članka 8. Povelje nužno ostvarivati prava u ravnoteži s drugim pravima. [25] Sljedećih nekoliko važnih primjera pokazuje kako se postiže ta ravnoteža.

1.2.1. Sloboda izražavanja

Jedno od prava koje može doći u sukob s pravom na zaštitu podataka jest pravo na slobodu izražavanja.

Sloboda izražavanja zaštićena je člankom 11. Povelje („Sloboda izražavanja i informiranja"). To pravo obuhvaća „slobodu mišljenja i slobodu primanja i davanja informacija i ideja bez uplitanja tijela vlasti i bez obzira na granice." Članak 11. odgovara članku 10. Konvencije. Sukladno članku 52. stavku 3. Povelje, u mjeri u kojoj sadrži prava koja odgovaraju pravima zajamčenim Europskom konvencijom o ljudskim pravima, „značenje i opseg primjene tih prava jednaki su onima iz spomenute Konvencije". Ograničenja koja se zakonito mogu nametnuti pravu zajamčenom u članku 11. Povelje stoga ne smiju premašiti ona iz članka 10. stavka 2. Konvencije, drugim riječima, moraju biti zakonom propisana i nužna u demokratskom društvu „radi zaštite [...] ugleda ili prava drugih." To načelo obuhvaća pravo na zaštitu podataka.

Odnos između zaštite osobnih podataka i slobode izražavanja reguliran je člankom 9. Direktive o zaštiti podataka naslovljenim „Obrada osobnih podataka i sloboda

25 ECtHR, *Von Hannover protiv Njemačke (br. 2)* [GC], br. 40660/08 i 60641/08, 7. veljače 2012.; CJEU, zajednički slučajevi 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. studenoga 2011., st. 48.; CJEU, C-275/06, *Productores de Música de España (Promusicae) protiv Telefónica de España SAU*, 29. siječnja 2008. st. 68. Vidjeti i Vijeće Europe (2013), sudska praksa Europskog suda za ljudska prava vezana uz zaštitu osobnih podataka, DP (2013) sudska praksa, dostupna na adresi: www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP%202013%20Case%20Law_Eng%20%28final%2018%2007%202013%29.pdf.

izražavanja".[26] Prema tom članku, države članice dužne su osigurati niz izuzeća ili ograničenja u pogledu zaštite podataka pa tako i u pogledu temeljnog prava na privatnost, navedenog u poglavljima II., IV. i VI. Direktive. Ta se izuzeća mogu činiti isključivo u novinarske svrhe ili u svrhe umjetničkog ili literarnog izražavanja, koji potpadaju pod područje primjene temeljnog prava na slobodu izražavanja, i to samo ako su nužna da bi se pravo na privatnost uskladilo s propisima koji reguliraju slobodu izražavanja.

Primjer: U predmetu *Tietosuojavaltuutettu protiv Satakunnan Markkinapörssi Oy i Satamedia Oy*,[27] od Suda Europske unije zatraženo je tumačenje članka 9. Direktive o zaštiti podataka kao i definicija odnosa između zaštite podataka i slobode tiska. Sud je morao ispitati slučaj objave poreznih podataka otprilike 1,2 milijuna fizičkih osoba koje su društva Markkinapörssi i Satamedia zakonito dobila od finskih poreznih tijela. Sud je prvenstveno trebao provjeriti treba li se obrada osobnih podataka, koje su porezna tijela stavila na raspolaganje kako bi se korisnicima mobilnih telefona omogućilo primanje poreznih podataka drugih fizičkih osoba, smatrati djelatnošću koja se provodi isključivo u novinarske svrhe. Zaključivši da su se djelatnosti Satakunnana sastojale od „obrade osobnih podataka" u smislu članka 3. stavka 1. Direktive o zaštiti podataka, Sud se usredotočio na tumačenje članka 9. Direktive. Sud se najprije osvrnuo na važnost prava na slobodu izražavanja u svakom demokratskom društvu držeći da se pojmovi vezani uz tu slobodu, poput novinarstva, trebaju široko tumačiti. Zatim je primijetio da se radi postizanja ravnoteže između dvaju temeljnih prava, izuzeća i ograničenja prava na zaštitu podataka moraju primjenjivati samo ako je to striktno neophodno. U tim je okolnostima Sud smatrao da se djelatnosti poput onih koje su provodili Markkinapörssi i Satamedia, a koje su se ticale podataka iz dokumenata u javnoj domeni u okviru nacionalnog zakonodavstva, mogu klasificirati kao „novinarske djelatnosti" ako je njihov predmet otkrivanje informacija, mišljenja i ideja javnosti, neovisno o mediju iskorištenom za njihov prijenos. Sud je također presudio da takve djelatnosti nisu ograničene na medijska društva i da se mogu obavljati u svrhe stjecanja profita. No, Sud je nacionalnom sudu prepustio odluku o tome je li tako bilo ovom konkretnom slučaju.

U pogledu usuglašavanja prava na zaštitu podataka i prava na slobodu izražavanja, Europski sud za ljudska prava donio je nekoliko orijentacijskih presuda.

26 Direktiva o zaštiti podataka, čl. 9.

27 CJEU, C-73/07, *Tietosuojavaltuutettu protiv Satakunnan Markkinapörssi Oy i Satamedia Oy*, 16. prosinca 2008., st. 56., 61. i 62.

Primjer: U predmetu *Axel Springer AG protiv Njemačke,*[28] Europski sud za ljudska prava smatrao je da je domaći sud svojom zabranom objavljivanja članka o uhićenju i osudi vrlo poznatog glumca vlasniku novina prekršio članak 10. Konvencije. Europski sud se ponovno pozvao na kriterij koji je utvrdio u svojoj sudskoj praksi u vezi uravnoteživanja prava na slobodu izražavanja i prava poštovanja privatnog života:

- prvo, je li događaj na koji se odnosio objavljeni članak bio od općeg interesa: uhićenje i osuda osobe je javna sudska činjenica te je stoga i od javnog interesa
- drugo, je li dotična osoba javna ličnost: dotična je osoba bio glumac koji je bio dovoljno poznat da bi se smatrao javnom ličnošću
- treće, kako su informacije dobivene i jesu li bile pouzdane: informacije je dostavio ured javnog tužitelja, a točnost informacija sadržanih u obje objave nije bila predmet spora između stranki.

Stoga je Sud za ljudska prava presudio da ograničenja objave nametnuta društvu nisu opravdano razmjerna zakonitom cilju zaštite privatnog života podnositelja. Sud je zaključio da je prekršen članak 10. Konvencije.

Primjer: U predmetu *Von Hannover protiv Njemačke (br. 2)*,[29] Europski sud za ljudska prava nije utvrdio kršenje prava na poštovanje privatnog života iz članka 8. Konvencije kada je princezi Caroline od Monaka odbijena sudska zabrana objave fotografije nje i njena supruga snimljene za vrijeme odmora na skijanju. Fotografija je objavljena uz članak koji se, među ostalim, bavio lošim zdravstvenim stanjem princa Rainiera. Sud za ljudska prava je zaključio da su domaći sudovi pažljivo odvagnuli pravo izdavačke tvrtke na slobodu izražavanja i pravo podnositelja na poštovanje privatnog života. Domaći sudovi su okarakterizirali bolest princa Rainiera kao događaj koji zanima moderno društvo što se nije moglo smatrati nerazumnim pa je Sud za ljudska prava mogao prihvatiti da je fotografija, razmotrena u kontekstu članka, ipak donekle doprinijela raspravi od općeg interesa. Sud je zaključio da nije prekršen članak 8. Konvencije.

28 ECtHR, *Axel Springer AG protiv Njemačke* [GC], br. 39954/08, 7. veljače 2012., st. 90. i 91.

29 ECtHR, *Von Hannover protiv Njemačke (br. 2)* [GC], br. 40660/08 i 60641/08, 7. veljače 2012., st. 118. i 124.

U sudskoj praksi Europskog suda za ljudska prava jedan je od ključnih kriterija koji se tiču uravnoteživanja prava kriterij doprinosa dotičnog izražavanja raspravi od općeg javnog interesa.

Primjer: U predmetu *Mosley protiv Ujedinjene Kraljevine*,[30] jedan je nacionalni tjednik objavio intimne fotografije podnositelja. Ovaj se zatim žalio na povredu članka 8. Konvencije jer nije mogao zatražiti sudsku zabranu prije objave dotičnih fotografija jer se novinama za objavu materijala kojim mogu prekršiti nečije pravo na privatnost ne postavljaju ikakvi uvjeti prethodnog obavještavanja. Iako je navedeni materijal objavljen općenito više u zabavne nego u obrazovne svrhe, nedvojbeno se podrazumijevala zaštita zajamčena člankom 10. Konvencije, te se takva objava mogla nadovezati na zahtjeve iz članka 8. Konvencije s obzirom na to da su informacije bile privatne i intimne naravi te nije bilo javnog interesa za njihovu objavu. Ovdje je ipak valjalo obratiti posebnu pažnju pri ispitivanju ograničenja koja se mogu smatrati oblikom cenzure prije objave. Zbog neugodnosti koje bi moglo prouzročiti postavljanje zahtjeva za prethodnim obavještavanjem, dvojbi o njegovoj učinkovitosti i velikog raspona procjena koje bi se njime otvorile u ovome području, Sud je zaključio da članak 8. ne zahtijeva pravno obvezujući zahtjev za prethodnim obavještavanjem. Shodno tome, Sud je zaključio da nije prekršen članak 8. Konvencije.

Primjer: U predmetu *Biriuk protiv Litve*,[31] podnositeljica je od dnevnih novina zahtijevala odštetu jer su objavile članak u kojem je pisalo da je HIV pozitivna. Tu su informaciju navodno potvrdili liječnici lokalne bolnice. Europski sud za ljudska prava smatrao je da dotični članak ne doprinosi raspravi od općeg interesa ponovivši da je zaštita osobnih podataka i to osobito medicinskih, od temeljne važnosti za ostvarenje pravo pojedinca na poštovanje privatnog i obiteljskog života, što je zajamčeno člankom 8. Konvencije. Sud je osobitu važnost pridao činjenici da je, sukladno novinskom članku, liječničko osoblje bolnice pružilo informacije o zarazi podnositeljice virusom HIV čime je očito prekršilo obvezu čuvanja liječničke tajne. Država dakle nije osigurala pravo podnositeljice na poštivanje njena privatnog života. Sud je zaključio da je prekršen članak 8.

30 ECtHR, *Mosley protiv Ujedinjene Kraljevine*, br. 48009/08, 10. svibnja 2011., st. 129. i 130.

31 ECtHR, *Biriuk protiv Litve*, br. 23373/03, 25. studenog 2008.

1.2.2. Pristup dokumentima

Sukladno članku 11. Povelje i članku 10. Konvencije, slobodom informiranja štiti se pravo ne samo na davanje već i na *primanje* informacija. Sve se više uviđa koliko je javna transparentnost važna za funkcioniranje demokratskog društva. Posljednja je dva desetljeća, shodno tome, pravo pristupa dokumentima javnih tijela potvrđeno kao važno pravo svakog građanina Unije te svake fizičke osobe koja prebiva odnosno pravne osobe sa sjedištem u nekoj državi članici.

Unutar prava Vijeća Europe može se pozvati na načela sadržana u Preporuci o pristupu službenim dokumentima koja je nadahnula autore Konvencije o pristupu službenim dokumentima *(Konvencija br. 205)*.[32] **Unutar prava Europske unije** pravo pristupa dokumentima zajamčeno je Uredbom 1049/2001 o javnom pristupu dokumentima Europskog parlamenta, Vijeća i Komisije (*Uredba o pristupu dokumentima*).[33] Člankom 42. Povelje i člankom 15. stavkom 3. Ugovora u funkcioniraju Europske unije to je pravo pristupa prošireno na pristup „dokumentima institucija, tijela, ureda i agencija Unije, neovisno o njihovu obliku". Sukladno članku 52. stavku 2. Povelje, pravo pristupa dokumentima također je ostvarivo pod uvjetima i u okviru ograničenja iz članka 15. stavka 3. Ugovora u funkcioniraju Europske unije. To pravo može biti u suprotnosti s pravom na zaštitu podataka ako se pristupom dokumentu otkrivaju osobni podaci pojedinca. Stoga može biti potrebno uravnotežiti zahtjeve pristupa dokumentima ili informacijama javnih tijela s pravom na zaštitu podataka osoba čiji su podaci sadržani u zatraženim dokumentima.

Primjer: U predmetu *Komisija protiv Bavarian Lager*,[34] Sud Europske unije definirao je područje primjene zaštite osobnih podataka u kontekstu pristupa dokumentima institucija Unije i odnosa između Uredbi br. 1049/2001 (*Uredba o pristupu dokumentima*) i 45/2001 (*Uredba o zaštiti podataka*). Društvo Bavarian Lager, osnovano 1992., uvozi njemačko pivo u bocama u Ujedinjenu Kraljevinu, prvenstveno za pivnice i barove. No, navedeno je društvo naišlo na prepreke jer je britansko zakonodavstvo *de facto* u povoljniji položaj stavljalo nacionalne proizvođače. Kao odgovor na žalbu društva Bavarian Lager, Europska komisija

32 Vijeće Europe, Odbor ministara (2002), Preporuka Rec(2002)2 državama članicama o pristupu službenim dokumentima, 21. veljače 2002.; Vijeće Europe, Konvencija o pristupu službenim dokumentima, CETS br. 205, 18. lipnja 2009. Konvencija još nije stupila na snagu.

33 Uredba (EZ) br. 1049/2001 Europskog parlamenta i Vijeća od 30 svibnja 2001. o javnom pristupu dokumentima Europskog parlamenta, Vijeća i Komisije, SL L 2001 L 145.

34 CJEU, C-28/08 P, *Europska komisija protiv The Bavarian Lager Co. Ltd*, 29. lipnja 2010., st. 60., 63., 76., 78. i 79.

odlučila je pokrenuti postupak protiv Ujedinjene Kraljevine jer nije ispunila svoju obvezu slijedom čega su izmijenjene osporavane odredbe koje su usklađene s pravom Europske unije. Bavarian Lager zatim je od Komisije među ostalim dokumentima zatražio i presliku zapisnika sa sastanka na kojem su sudjelovali predstavnici Komisije, britanskih nadležnih tijela i *Confédération des Brasseurs du Marché Commun* (CBMC). Komisija je pristala otkriti određene dokumente vezane uz sastanak, no izostavila je pet imena koja su se pojavljivala u zapisniku jer su se dvije osobe izričito protivile otkrivanju identiteta, a Komisija nije uspjela kontaktirati s ostala tri sudionika. Odlukom od 18. ožujka 2004. Komisija je odbila novu predstavku kojom je društvo Bavarian Lager tražilo cjeloviti zapisnik sa sastanka pozivajući se prvenstveno na zaštitu privatnog života pojedinaca zajamčenu Uredbom o zaštiti podataka. Budući da nije bilo zadovoljno iznesenim stavom, društvo Bavarian Lager podnijelo je tužbu Prvostupanjskom sudu koji je poništio odluku Komisije presudom od 8. studenoga 2007. (slučaj T-194/04, *Bavarian Lager protiv Komisije*), smatrajući u prvom redu da samo navođenje imena dotičnih osoba koje su predstavljale određena tijela na popisu sudionika sastanka ne predstavlja narušavanje privatnog života niti dovodi privatne živote tih osoba u bilo kakvu opasnost.

Na žalbu Komisije, Sud Europske unije poništio je presudu Prvostupanjskog suda. Sud je smatrao da se Uredbom o pristupu dokumentima utvrđuje „konkretan ojačani sustav zaštite pojedinca čiji se osobni podaci, u određenim slučajevima, mogu priopćiti javnosti". Prema Sudu, kada se zahtjevom koji se zasniva na Uredbi o pristupu dokumentima traži pristup dokumentima koji uključuju osobne podatke, u cijelosti se primjenjuju odredbe Uredbe o zaštiti podataka. Sud je zatim zaključio da je Komisija s pravom odbila predstavku za pristup cjelovitom sadržaju zapisnika sa sastanka iz listopada 1996. U nedostatku suglasnosti petero sudionika sastanka, Komisija je u dovoljnoj mjeri ispunila svoju dužnost otvorenosti dostavljajući verziju dokumenta u kojoj su izostavljena njihova imena.

Nadalje, prema Sudu, „kako Bavarian Lager nije izričito i legitimno opravdao svoj zahtjev niti je pružio ikakav uvjerljiv argument kojim bi dokazao nužnost dostave tih osobnih podataka, Komisija nije mogla odvagnuti razne interese dotičnih stranki, niti je mogla provjeriti je li bilo razloga za pretpostavku da se mogu ugroziti legitimni interesi osoba čiji se podaci obrađuju", kako se zahtijeva Uredbom o zaštiti podataka.

Prema ovoj presudi, za zadiranje u pravo na zaštitu podataka vezano uz pristup dokumentima treba postojati konkretan i opravdan razlog. Pravo na pristup dokumentima ne može automatski nadjačati pravo na zaštitu podataka.[35]

Posebnim aspektom zahtjeva za pristup bavila se sljedeća presuda Europskog suda za ljudska prava.

> Primjer: U predmetu *Társaság a Szabadságjogokért protiv Mađarske*,[36] podnositelj, nevladina organizacija za ljudska prava, od Ustavnog suda tražio je pristup informacijama o slučaju u tijeku. Bez prethodnog savjetovanja s parlamentarcem koji mu je podnio tužbu, Ustavni sud odbio je zahtjev za pristupom s obrazloženjem da se žalbe koje su mu podnesene mogu staviti na raspolaganje trećim osobama samo uz odobrenje podnositelja. Domaći sudovi potvrdili su ovu uskratu uz obrazloženje da zaštitu takvih osobnih podataka ne mogu nadjačati drugi zakoniti interesi, uključujući dostupnost javnih informacija. Podnositelj je bio u službi „čuvara društva", čije su aktivnosti jamčile sličnu zaštitu poput one koju uživa tisak. Vezano uz slobodu tiska, Sud za ljudska prava bio je dosljedan u svojem stajalištu da javnost ima pravo na informacije od općeg interesa. Informacije koje je podnositelj tražio bile su „spremne i dostupne" i nisu zahtijevale bilo kakvo prikupljanje podataka. U tim je okolnostima država bila dužna ne opstruirati prijenos informacija koje je zatražio podnositelj. Ukratko, Sud za ljudska prava smatrao je da prepreke kojima se ometa pristup informacijama od javnog interesa mogu ometati medijske i srodne djelatnike u vršenju njihove vitalne uloge „javnih čuvara". Sud je zaključio da je prekršen članak 10.

Prema pravu Europske unije jasno je utvrđena važnost transparentnosti. Načelo transparentnosti sadržano je u člancima 1. i 10. Ugovora o Europskoj uniji i u članku 15. stavku 1. Ugovora u funkcioniraju Europske unije.[37] Prema uvodnoj izjavi 2. Uredbe (EZ) br. 1049/2001, to načelo građanima omogućuje aktivnije

35 Na ovu temu ipak pogledati detaljne rasprave Europskog nadzornika za zaštitu podataka (EDPS) (2011), *Javni pristup dokumentima koji sadrže osobne podatke nakon presude društvu* Bavarian Lager, Bruxelles, 24. ožujka 2011., dostupne na adresi: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

36 ECtHR, *Társaság a Szabadságjogokért protiv Mađarske*, br. 37374/05, 14. travnja 2009.; vidjeti st. 27., 36.–38.

37 EU (2012), Pročišćene verzije Ugovora o Europskoj uniji i Ugovora o funkcioniranju Europske unije, SL L 2012 C 326.

sudjelovanje u postupku odlučivanja, jamčeći im legitimniju, učinkovitiju i odgovorniju administraciju u demokratskom sustavu.[38]

Slijedom navedenoga, Uredbom Vijeća (EZ) br. 1290/2005 o financiranju zajedničke poljoprivredne politike i Uredbom Komisije (EZ) br. 259/2008 o detaljnim pravilima njene primjene zahtijeva se objava informacija o korisnicima određenih sredstava Europske unije u poljoprivrednom sektoru te o iznosima koje je svaki korisnik primio.[39] Objavljivanje takvih informacija trebalo bi doprinijeti javnoj kontroli administracije u pogledu odgovarajuće uporabe javnih sredstava. Nekoliko je korisnika osporilo razmjernost takve objave.

Primjer: U predmetu *Volker i Markus Schecke i Hartmut Eifert protiv Land Hessen*,[40] Sud Europske unije morao je prosuditi razmjernost objave imena korisnika poljoprivrednih subvencija Europske unije te iznosa koje je svaki od njih primio, kako nalaže zakonodavstvo Europske unije.

Napominjući da pravo na zaštitu podataka nije apsolutno pravo, Sud je smatrao da je objava podataka o imenima korisnika dvaju poljoprivrednih fondova Unije s ukupnim iznosima primljenih potpora na internetskoj stranici zadiranje u privatni život korisnika, a osobito u zaštitu njihovih osobnih podataka.

Sud je smatrao da je takvo zadiranje u članke 7. i 8. Povelje omogućeno zakonom te da je njime ispunjen cilj općeg interesa koji Unija priznaje, a koji uključuje transparentnije korištenje fondova zajednice. Unatoč tome, Sud je bio mišljenja da je objava imena fizičkih osoba korisnika poljoprivredne potpore Unije iz spomenuta dva fonda te ukupnih iznosa koje su primili nerazmjerna i neopravdana mjera uzimajući u obzir članak 52. stavak 1. Povelje. Sud je stoga zakonodavstvo Europske unije o objavi informacija o korisnicima europskih poljoprivrednih fondova proglasio djelomično nevaljanim.

38 CJEU, C-41/00 P, *Interporc Im- und Export GmbH protiv Komisije Europskih zajednica*, 6. ožujka 2003., st. 39.; i CJEU, C-28/08 P, *Europska komisija protiv The Bavarian Lager Co. Ltd*, 29. lipnja 2010., st. 54.

39 Uredba Vijeća (EZ) br. 1290/2005 od 21. lipnja 2005. o financiranju zajedničke poljoprivredne politike, SL L 2005 L 209; i Uredba Komisije (EZ) br. 259/2008 od 18. ožujka 2008. o detaljnim pravilima primjene Uredbe Vijeća (EZ) br. 1290/2005 u pogledu objave informacija o korisnicima sredstava Europskog fonda za jamstva u poljoprivredi (EAGF) i Europskog poljoprivrednog fonda za ruralni razvoj (EAFRD), SL L 2008 L 76.

40 CJEU, zajednički slučajevi C-92/09 i C-93/09, *Volker i Markus Schecke GbR (C-92/09) i Hartmut Eifert (C-93/09) protiv Land Hessen*, 9. studenoga 2010., st. 47.–52., 58., 66.–67., 75., 86. i 92.

1.2.3. Sloboda umjetnosti i znanosti

Sloboda umjetnosti i znanosti, koja je izričito zaštićena člankom 13. Povelje, predstavlja još jedno pravo koje valja uravnotežiti s pravom na poštovanje privatnog života i zaštitu podataka. To je pravo u prvom redu izvedeno iz prava na slobodu mišljenja i izražavanja, a njegovo uživanje podliježe članku 1. Povelje (ljudsko dostojanstvo). Europski sud za ljudska prava smatra da je sloboda umjetnosti zaštićena člankom 10. Europske konvencije o ljudskim pravima.[41] Pravo zajamčeno člankom 13. Povelje može podlijegati ograničenjima iz članka 10. Konvencije.[42]

Primjer: U predmetu *Vereinigung bildender Künstler protiv Austrije*,[43] austrijski sudovi zabranili su udruzi podnositeljici daljnje izlaganje slike s fotografijama glava različitih javnih ličnosti u seksualnim pozama. Austrijski parlamentarac čija je fotografija također iskorištena na slici pokrenuo je postupak protiv udruge podnositeljice tražeći zabranu izlaganja slike. Domaći je sud prihvatio njegov zahtjev i dosudio zabranu. Europski sud za ljudska prava ponovio je da se članak 10. Konvencije primjenjuje na širenje ideja koje vrijeđaju, izazivaju šok ili uznemiruju državu ili bio koji dio populacije. Oni koji stvaraju, izvode, šire ili izlažu umjetnička djela doprinose razmjeni ideja i mišljenja i država je dužna ne uskratiti im nepotrebno slobodu izražavanja. Budući da je predmetna slika bila kolaž u kojem su iskorištene samo glave osoba, a njihova su tijela oslikana na nerealističan i pretjeran način, čija svrha očito nije bila predstavljanje pa čak ni nagovještaj stvarnosti, Sud za ljudska prava nadalje je izjavio da „se slika teško može tumačiti kao da se tiče privatnog života [dotičnog], već se ona prije tiče njegova javnog položaja političara" te da je „u tom svojstvu [dotični] trebao pokazati više tolerancije na kritiku". Odvagujući različite interese, Sud je zaključio da je neograničena zabrana daljnjeg izlaganja slike nerazmjerna. Sud je zaključio da je prekršen članak 10. Konvencije.

Kada je posrijedi znanost, europsko zakonodavstvo o zaštiti podataka uzima u obzir posebnu vrijednost koju ona ima za društvo. Iz tog su razloga smanjena opća ograničenja uporabe osobnih podataka. I Direktiva o zaštiti podataka i Konvencija br. 108. dopuštaju zadržavanje podataka za znanstvena istraživanja i kada više nisu potrebni u prvobitne svrhe za koje su prikupljeni. Isto se tako ni daljnja uporaba osobnih

41 ECtHR, *Müller i drugi protiv Švicarske*, br. 10737/84, 24. svibnja 1988.

42 Objašnjenja vezana uz Povelju o temeljnim pravima, SL L 2007 C 303.

43 ECtHR, *Vereinigung bildender Künstler protiv Austrije*, br. 68345/01, 25. siječnja 2007.; vidjeti osobito st. 26. i 34.

podataka u znanstvenim istraživanjima ne smatra neprikladnom svrhom. Zadaća je nacionalnog prava donijeti detaljnije odredbe, uključujući nužne mjere zaštite, kojima će se pomiriti interes znanstvenih istraživanja i prava na zaštitu podataka (vidjeti i odjeljke 3.3.3 i 8.4).

1.2.4. Zaštita vlasništva

Pravo na zaštitu vlasništva sadržano je u članku 1. Prvog protokola uz Europsku konvenciju o ljudskim pravima te u članku 17. stavku 1. Povelje. Jedan od važnih aspekata prava na vlasništvo jest zaštita intelektualnog vlasništva koja se izričito spominje u članku 17. stavku 2. Povelje. U pravnom poretku Europske unije postoji nekoliko direktiva donesenih u svrhu učinkovite zaštite intelektualnog vlasništva i to osobito autorskog prava. Intelektualno vlasništvo ne obuhvaća samo literarno i umjetničko vlasništvo, već i patente, žigove i srodna prava.

Iz sudske prakse Suda Europske unije jasno proizlazi da se zaštita temeljnog prava na vlasništvo mora uravnotežiti sa zaštitom drugih temeljnih prava, osobito prava na zaštitu podataka.[44] Bilo je slučajeva kada su institucije za zaštitu autorskih prava od davatelja internetskih usluga tražile da otkriju identitet korisnika internetskih platformi za zajedničko korištenje datoteka. Takve platforme naime korisnicima interneta često omogućuju besplatno preuzimanje glazbenih zapisa unatoč tome što su zaštićeni autorskim pravom.

Primjer: *Predmet Promusicae protiv Telefónica de España*[45] ticao se protivljenja španjolskog pružatelja usluge internetskog pristupa, društva Telefónica, otkrivanju osobnih podataka nekolicine osoba kojima je pružao usluge internetskog pristupa neprofitnoj organizaciji glazbenih producenata i izdavača glazbenih i audiovizualnih snimki pod nazivom Promusicae. Organizacija Promusicae zatražila je otkrivanje informacija kako bi mogla pokrenuti građanski postupak protiv tih osoba, za koje je tvrdila da su koristile program razmjene datoteka s pristupom fonogramima na koje su pravo upotrebe polagali članovi Promusicae.

Španjolski je sud predmet proslijedio Sudu Europske unije zatraživši odgovor na pitanje moraju li se, prema pravu zajednice, takvi osobni podaci priopćiti u kontekstu građanskih parnica kako bi se osigurala učinkovita zaštita autorskog

44 ECtHR, *Ashby Donald i drugi protiv Francuske*, br. 36769/08, 10. siječnja 2013.

45 CJEU, C-275/06, *Productores de Música de España (Promusicae) protiv Telefónica de España SAU*, 29. siječnja 2008., st. 54. i 60.

prava. Pozvao se na Direktive 2000/31, 2001/29 i 2004/48, tumačene i u svjetlu članaka 17. i 47. Povelje. Sud je zaključio da ove tri direktive, kao i Direktiva o e-privatnosti (Direktiva 2002/58), ne sprečavaju države članice da propišu obvezu otkrivanja osobnih podataka u kontekstu građanskih parnica, radi učinkovite zaštite autorskog prava.

Sud je istaknuo da je slučaj potaknuo pitanje potrebe za usklađivanjem zahtjeva za zaštitom različitih temeljnih prava, odnosno prava na poštovanje privatnog života i prava na zaštitu vlasništva i djelotvoran pravni lijek.

Sud je zaključio da se „države članice pri prenošenju gore navedenih direktiva moraju oslanjati na ono njihovo tumačenje koje će omogućiti pravednu ravnotežu različitih temeljnih prava zaštićenih pravnim poretkom Zajednice. Nadalje, pri provedbi mjera kojima se navedene direktive prenose, nadležna tijela i sudovi država članica ne moraju samo tumačiti svoje nacionalno pravo dosljedno s direktivama, već i osigurati da se ne oslanjaju na njihovo tumačenje koje bi bilo u sukobu s navedenim temeljnim pravima ili drugim općim načelima prava Zajednice, kao što je načelo razmjernosti."[46]

46 *Ibid.*, st. 65. i 68.; vidjeti i CJEU, C-360/10, *SABAM protiv Netlog N.V.*, 16. veljače 2012.

2

Terminologija vezana uz zaštitu podataka

EU	Pitanja kojima se bavi	Vijeće Europe
Osobni podaci		
Direktiva o zaštiti podataka, članak 2. točka (a) CJEU, zajednički slučajevi C-92/09 i C-93/09, *Volker i Markus Schecke GbR (C-92/09) i Hartmut Eifert (C-93/09) protiv Land Hessen*, 9. studenoga 2010. CJEU, C-275/06, *Productores de Música de España (Promusicae) protiv Telefónica de España SAU*, 29. siječnja 2008.	**Pravna definicija**	Konvencija br. 108, članak 2. točka (a) ECtHR, *Bernh Larsen Holding AS i drugi protiv Norveške*, br. 24117/08, 14. ožujka 2013.
Direktiva o zaštiti podataka, članak 8. stavak 1. CJEU, C-101/01, *Bodil Lindqvist*, 6. studenoga 2003.	**Posebne kategorije osobnih podataka (osjetljivi podaci)**	Konvencija br. 108, članak 6.
Direktiva o zaštiti podataka, članak 6. stavak 1. točka (e)	**Anonimizirani i pseudonimizirani podaci**	Konvencija br. 108, članak 5. točka (e) Konvencija br. 108, Eksplanatorno izvješće, članak 42.
Obrada podataka		
Direktiva o zaštiti podataka, članak 2. točka (b) CJEU, C-101/01, *Bodil Lindqvist*, 6. studenoga 2003.	**Definicije**	Konvencija br. 108, članak 2. točka (c)

EU	Pitanja kojima se bavi	Vijeće Europe
Korisnici podataka		
Direktiva o zaštiti podataka, članak 2. točka (d)	**Nadzornik**	Konvencija br. 108, članak 2. točka (d) Preporuka o profiliranju, članak 1. točka (g) *
Direktiva o zaštiti podataka, članak 2. točka (e) CJEU, C-101/01, *Bodil Lindqvist*, 6. studenoga 2003.	**Obrađivač**	Preporuka o profiliranju, članak 1. točka (h)
Direktiva o zaštiti podataka, članak 2. točka (g)	**Primatelj**	Konvencija br. 108, Dodatni protokol, članak 2. stavak 1.
Direktiva o zaštiti podataka, članak 2. točka (f)	**Treća stranka**	
Suglasnost		
Direktiva o zaštiti podataka, članak 2. točka (h) CJEU, C-543/09, *Deutsche Telekom AG protiv Bundesrepublik Deutschland*, 5. svibnja 2011.	**Definicije i zahtjevi za valjanu suglasnost**	Preporuka o medicinskim podacima, članak 6., i razne naknadne preporuke

*Napomena: * Vijeće Europe, Odbor ministara (2010), Preporuka Rec(2010)13 državama članicama u zaštiti pojedinaca pri automatskoj obradi osobnih podataka u kontekstu profiliranja (Preporuka o profiliranju), 23. studenoga 2010.*

2.1. Osobni podaci

Ključne točke

- Podaci su osobni ako se odnose na osobu utvrđenog identiteta ili osobu čiji se identitet može utvrditi, odnosno osobu čiji se podaci obrađuju.
- Osoba se može identificirati ako se bez značajnijeg napora mogu dobiti informacije o njoj, čime se omogućuje identifikacija osobe čiji se podaci obrađuju.
- Autentikacija je postupak dokazivanja da određena osoba ima određeni identitet i/ili je ovlaštena za poduzimanje određenih radnji.
- Postoje posebne kategorije podataka, takozvani osjetljivi podaci, navedeni u Konvenciji br. 108 i u Direktivi o zaštiti podataka, koji zahtijevaju pojačanu zaštitu te stoga podliježu posebnom pravnom režimu.

- Podaci su anonimizirani ako više ne sadrže identifikatore, a pseudonimizirani ako su identifikatori kodirani.
- Za razliku od anonimiziranih podataka, pseudonimizirani podaci su osobni podaci.

2.1.1. Glavni aspekti pojma osobnih podataka

Temeljem prava Europske unije kao i **temeljem prava Vijeća Europe**, „osobni podaci" definirani su kao informacije koje se odnose na identificiranu fizičku osobu ili fizičku osobu koju se može identificirati,[47] to jest informacije o osobi čiji je identitet sasvim jasan ili ga je barem moguće utvrditi uz dodatne informacije.

Ako se podaci o takvoj osobi obrađuju, ona se naziva „osoba čiji se podaci obrađuju".

Osoba

Pravo na zaštitu podataka razvilo se iz prava na poštovanje privatnog života. Pojam privatnog života odnosi se na ljudska bića pa su s time u skladu fizičke osobe primarni korisnici zaštite podataka. Nadalje, sukladno Mišljenju radne skupine iz članka 29., samo je *živo biće* zaštićeno europskim zakonodavstvom o zaštiti podataka.[48]

Sudska praksa Europskog suda za ljudska prava koja se odnosi na članak 8. Europske konvencije o ljudskim pravima ukazuje na to kako može biti teško potpuno razdvojiti privatni i profesionalni život.[49]

Primjer: U predmetu *Amann protiv Švicarske*,[50] službene su vlasti prisluškivale poslovni telefonski razgovor podnositelja. Na temelju tog razgovora vlasti su istražile podnositelja i ispunile karticu podnositelja za kartični indeks nacionalne sigurnosti. Iako se prisluškivanje odnosilo na poslovni telefonski razgovor, sa stajališta Suda za ljudska prava pohrana podataka o pozivu odnosila se na privatni život podnositelja. Sud je istaknuo da se pojam „privatni život" ne smije

47 Direktiva o zaštiti podataka, čl. 2. točka (a); Konvencija br. 108, čl. 2. točka (a).

48 *Mišljenje 4/2007 o pojmu osobnih podataka* Radne skupine iz članka 29. (2007.), WP 136, 20. lipnja 2007., str. 22.

49 Vidjeti primjerice ECtHR, *Rotaru protiv Rumunjske* [GC], br. 28341/95, 4. svibnja 2000., st. 43.; ECtHR, *Niemitz protiv Njemačke*, 13710/88, 16. prosinca 1992., st. 29.

50 ECtHR, *Amann protiv Švicarske* [GC], br. 27798/95, 16. veljače 2000., st. 65.

tumačiti restriktivno i to poglavito stoga što poštovanje privatnog života sadrži pravo na uspostavljanje i razvijanje odnosa s drugim ljudskim bićima. Nadalje, nije bilo ikakvog načelnog razloga kako bi se opravdalo izuzimanje radnji profesionalne ili poslovne prirode iz pojma „privatnog života". Takvo široko tumačenje odgovaralo je onome iz Konvencije br. 108. Sud je nadalje držao da uplitanje u slučaj podnositelja nije bilo u skladu sa zakonom, jer nacionalno zakonodavstvo nije sadržavalo konkretne i detaljne odredbe o prikupljanju, snimanju i pohrani informacija. Sud je stoga zaključio da je prekršen članak 8. Konvencije.

Ako i pitanja profesionalnog života mogu biti predmetom zaštite podataka, upitno je zašto se zaštita nudi samo fizičkim osobama. Prava se sukladno Europskoj konvenciji o ljudskim pravima jamče ne samo fizičkim osobama, već svima.

Postoji sudska praksa Europskog suda za ljudska prava s presudama u tužbama pravnih osoba zbog navodnog kršenja prava na zaštitu od uporabe njihovih podataka sukladno članku 8. Konvencije. No sud je slučaj promatrao iz perspektive prava na poštovanje doma i dopisivanja, a ne privatnog života:

Primjer: Predmet *Bernh Larsen Holding AS i drugi protiv Norveške*[51] ticao se žalbe triju norveških društava na odluku poreznog tijela koja im je nalagala da poreznim revizorima dostave preslike svih podataka s računalnog poslužitelja koji su sva tri društva zajednički koristila.

Europski sud za ljudska prava smatrao je da je takva obveza nametnuta društvima podnositeljima bila zadiranje u njihova prava na poštovanje „doma" i „dopisivanja" u svrhe članka 8. Konvencije. No, Sud je zaključio da su porezna tijela raspolagala odgovarajućim i učinkovitim mehanizmima zaštite od zloporabe: društva podnositelji obaviještena su dovoljno vremena unaprijed; bila su prisutna i mogla su sudjelovati u postupku tijekom intervencije na licu mjesta; a materijal se trebao uništiti po završetku porezne revizije. U tim je okolnostima postignuta pravedna ravnoteža između prava društava podnositelja na poštovanje „doma" i „dopisivanja" te njihova interesa vezanog uz zaštitu privatnosti njihovih zaposlenika s jedne strane, i javnog interesa učinkovite inspekcije radi porezne procjene s druge strane. Sud je zaključio da stoga nije prekršen članak 8.

51 ECtHR, *Bernh Larsen Holding AS i drugi protiv Norveške*, br. 24117/08, 14. ožujka 2013. Vidjeti i ECtHR, *Liberty i drugi protiv Ujedinjene Kraljevine*, br. 58243/00, 1. srpnja 2008.

Prema Konvenciji br. 108, zaštita podataka u prvom se redu bavi zaštitom fizičkih osoba; no ugovorne stranke u okviru nacionalnog zakonodavstva mogu proširiti zaštitu podataka i na pravne osobe, primjerice poslovna društva i udruge. **Europsko zakonodavstvo o zaštiti podataka** u načelu ne pokriva zaštitu pravnih osoba u pogledu obrade s njima povezanih podataka. Nacionalni zakonodavci slobodno mogu regulirati to pitanje.[52]

Primjer: U predmetu *Volker i Markus Schecke i Hartmut Eifert protiv Land Hessen*,[53] Sud Europske unije, pozivajući se na objavu osobnih podataka o korisnicima poljoprivredne potpore, smatrao je da „pravne osobe mogu tražiti zaštitu iz članaka 7. i 8. Povelje u odnosu na takvu identifikaciju samo ako službeni naziv pravne osobe identificira jednu fizičku osobu ili više njih. [...] pravo na poštovanje privatnog života vezano uz obradu osobnih podataka iz članaka 7. i 8. Povelje, tiče se bilo koje informacije koja se odnosi na identificiranog pojedinca ili pojedinca koji se može identificirati [...]".[54]

Mogućnost identifikacije osobe

Unutar prava Europske unije kao i **unutar prava Vijeća Europe**, informacije sadrže podatke o osobi ako:

- se pojedinac identificira kroz te informacije
- je pojedinac, unatoč tome što nije identificiran, opisan kroz te informacije na način koji omogućuje otkrivanje osobe čiji se podaci obrađuju dodatnim istraživanjem.

Obje su ove vrste informacija na isti način zaštićene europskim zakonodavstvom o zaštiti podataka. Europski sud za ljudska prava često je ponavljao da je pojam „osobnih podataka" prema Europskoj konvenciji o ljudskim pravima isti kao u Konvenciji br. 108, osobito što se tiče uvjeta koji se odnosi na identificirane osobe ili osobe koje je moguće identificirati.[55]

52 Direktiva o zaštiti podataka, uvodna izjava 24.

53 CJEU, zajednički slučajevi C-92/09 i C-93/09, *Volker i Markus Schecke GbR (C-92/09) i Hartmut Eifert (C-93/09) protiv Land Hessen*, 9. studenoga 2010., st. 53.

54 *Ibid.*, st. 52.

55 Vidjeti ECtHR, *Amann protiv Švicarske* [GC], br. 27798/95, 16. veljače 2000., st. 65. i *drugi*.

Pravne definicije osobnih podataka ne razjašnjavaju dalje kada se osoba smatra identificiranom.[56] Identifikacija očito podrazumijeva elemente koji osobu opisuju na način koji je razlikuje od svih drugih osoba i prepoznaje kao pojedinca. Ime osobe prvi je primjer takvih elemenata opisa. U iznimnim slučajevima drugi identifikatori mogu imati učinak sličan učinku imena. Kod javnih osoba primjerice može biti dovoljno uputiti na funkciju osobe, npr. predsjednik Europske komisije.

Primjer: U predmetu *Promusicae*,[57] Sud Europske unije izjavio je da „je neosporno da dostavljanje imena i adresa pojedinih korisnika [određene internetske platforme za zajedničko korištenje datoteka] koje je zatražila organizacija Promusicae uključuje stavljanje na raspolaganje osobnih podataka, odnosno informacija koje se tiču identificiranih fizičkih osoba ili fizičkih osoba koje je moguće identificirati, u skladu s definicijom iz članka 2. točke (a) Direktive 95/46 [...]. Takvo dostavljanje informacija koje je, kako je iznijela Promusicae, a Telefónica nije osporila, Telefónica pohranila, predstavlja obradu osobnih podataka u smislu prvog stavka članka 2. Direktive 2002/58, u vezi s člankom 2. točkom (b) Direktive 95/46".

Budući da mnoga imena nisu jedinstvena, za utvrđivanje identiteta osobe mogu biti potrebni dodatni identifikatori kako bi se osiguralo da se osoba ne zamijeni nekim drugim. Često se koriste datum i mjesto rođenja. U pojedinim su zemljama također uvedeni personalizirani brojevi kako bi se građani bolje međusobno razlikovali. Biometrijski podaci, kao što su otisci prstiju, digitalne fotografije ili skeniranja šarenice oka, sve su važniji za identificiranje osoba u tehnološko doba.

No preduvjet za primjenjivost europskog zakonodavstva o zaštiti podataka nije precizna identifikacija osobe čiji se podaci obrađuju; dovoljno je da se dotična osoba može identificirati. Smatra se da se osoba može identificirati ako informacije o njoj sadrže elemente identifikacije na temelju kojih se osoba može identificirati, izravno ili neizravno.[58] Sukladno uvodnoj izjavi 26. Direktive o zaštiti podataka, to se procjenjuje na temelju vjerojatnosti da će predvidivim korisnicima informacija biti dostupni prihvatljivi instrumenti identifikacije i da će ih korisnici poduzeti, što uključuje i primatelje treće stranke (vidjeti odjeljak 2.3.2).

56 Vidjeti i ECtHR, *Odièvre protiv Francuske* [GC], br. 42326/98, 13. veljače 2003.; i ECtHR, *Godelli protiv Italije*, br. 33783/09, 25. rujna 2012.

57 CJEU, C-275/06, *Productores de Música de España (Promusicae) protiv Telefónica de España SAU*, 29. siječnja 2008., st. 45.

58 Direktiva o zaštiti podataka, čl. 2. točka (a)

Primjer: Lokalno tijelo odluči prikupljati podatke o vozilima koja prebrzo prometuju lokalnim cestama. Potom fotografira vozila, automatski snimajući vrijeme i lokaciju, kako bi te podatke proslijedilo nadležnom tijelu radi kažnjavanja prijestupnika. Osoba čiji se podaci obrađuju uloži žalbu tvrdeći da lokalno tijelo, sukladno zakonodavstvu o zaštiti podataka, nema pravne osnove za takvo prikupljanje podataka. Lokalno tijelo smatra da ne prikuplja osobne podatke, tvrdeći da su podaci o registraciji podaci o anonimnim osobama. Lokalno tijelo nema pravnu ovlast pristupa općem registru vozila za otkrivanje identiteta vlasnika vozila ili vozača.

Taj se argument ne podudara s uvodnom izjavom 26. Direktive o zaštiti podataka. S obzirom na to da je očita svrha prikupljanja podataka identificirati i kazniti prekršitelje, izgledno je da će se pokušati izvršiti identifikacija. Premda lokalna tijela nemaju izravan pristup instrumentima identifikacije, oni podatke prosljeđuju nadležnom tijelu, odnosno policiji, koja raspolaže tim instrumentima. Iz uvodne izjave 26. također jasno proizlazi scenarij prema kojem se može predvidjeti da daljnji primatelji podataka, osim neposrednog korisnika podataka, mogu pokušati identificirati pojedinca. U svjetlu uvodne izjave 26., radnja koju je poduzelo lokalno tijelo izjednačena je s prikupljanjem podataka o osobama koje se mogu identificirati te je stoga za nju, sukladno zakonodavstvu o zaštiti podataka, potrebna pravna osnova.

Unutar prava Vijeća Europe mogućnost identifikacije tumači se na sličan način. U članku 1. stavku 2. Preporuke o podacima o plaćanjima,[59] navodi se primjerice da se osoba ne smatra „osobom koja se može identificirati" ako je za njenu identifikaciju potrebno uložiti previše vremena, financijskih sredstava ili radne snage.

Autentikacija

Autentikacija je postupak u kojem osoba može dokazati da posjeduje određeni identitet i/ili da je ovlaštena za određene radnje, poput pristupanja sigurnosnim područjima ili podizanja novca s bankovnog računa. Autentikacija se može provesti usporedbom biometrijskih podataka, kao što su fotografija ili otisak prsta u putovnici, s podacima kojima se osoba predstavlja prilikom, na primjer, imigracijske kontrole; ili traženjem podataka koje bi trebala znati samo osoba određenog identiteta ili s određenom ovlašću, kao što je jedinstveni identifikacijski broj (PIN) ili lozinka;

59 CoE, Odbor ministara (1990), Preporuka br. R Rec(90) 19 o zaštiti osobnih podataka korištenih za plaćanje i druge srodne radnje, 13. rujna 1990.

ili traženjem predočenja određenog tokena koji bi trebao biti u isključivom posjedu osobe određenog identiteta ili s određenom ovlašću, kao što su posebna čip kartica ili ključ bankovnog sefa. Osim lozinki ili čip kartica, katkad zajedno s PIN-ovima, elektronički potpis predstavlja vrlo učinkovit instrument identifikacije i autentikacije osobe u elektroničkim komunikacijama.

Priroda podataka

Svaka informacija može biti osobni podatak pod uvjetom da se odnosi na osobu.

> Primjer: Procjena radnih sposobnosti djelatnika koju nadređeni pohranjuje u osobni dosje djelatnika predstavlja osobni podatak o djelatniku unatoč tome što može sadržavati, djelomice ili u cijelosti, samo osobno mišljenje nadređenog, primjerice: „djelatnik nije posvećen poslu", a ne tvrde činjenice kao što su: „djelatnik je u proteklih šest mjeseci s posla izostao pet tjedana".

Osobni podaci obuhvaćaju informacije koje se tiču privatnog života osobe kao i informacije o profesionalnom ili javnom životu te osobe.

U predmetu pod nazivom *Slučaj Amann*,[60] Europski sud za ljudska prava pojam „osobni podaci" tumačio je ne ograničavajući ga na pitanja privatne sfere pojedinca (vidjeti odjeljak 2.1.1). Značenje pojma „osobni podaci" također je bitno za Direktivu o zaštiti podataka:

> Primjer: U predmetu *Volker i Markus Schecke i Hartmut Eifert protiv Land Hessen*,[61] Sud Europske unije izjavio je da „u tom smislu nije važno što se objavljeni podaci tiču radnji profesionalne prirode [...]. Europski sud za ljudska prava, pozivajući se na tumačenje članka 8. Konvencije, o ovom je pitanju zauzeo stav da pojam „privatni život" ne treba tumačiti restriktivno te da nema ikakvog načelnog razloga kako bi se opravdalo izuzimanje radnji profesionalne ... prirode iz pojma „privatnog života".

Podaci se odnose na osobe i ako sadržaj informacija neizravno otkriva podatke o osobi. U pojedinim slučajevima, kada postoji uska veza između predmeta ili događaja

60 Vidjeti ECtHR, *Amann protiv Švicarske* [GC], 16. veljače 2000., st. 65.

61 Zajednički slučajevi C-92/09 i C-93/09, *Volker i Markus Schecke GbR i Hartmut Eifert protiv Land Hessen*, 9. studenoga 2010., st. 59.

– npr. mobilnog telefona, automobila, nesreće – s jedne strane, i osobe – npr. kao vlasnika, korisnika, žrtve – s druge strane, informacije o predmetu ili događaju također se trebaju smatrati osobnim podacima.

Primjer: U predmetu *Uzun protiv Njemačke*,[62] podnositelj i još jedna osoba nadzirani su uređajem globalnog sustava pozicioniranja (GPS) koji je postavljen u automobil te druge osobe zbog sumnje da su uključeni u bombaške napade. U ovom je slučaju Europski sud za ljudska prava smatrao da je motrenje podnositelja preko GPS-a predstavljalo zadiranje u njegov privatni život zaštićen člankom 8. Konvencije. Ipak, nadzor putem GPS-a bio je u skladu sa zakonom te razmjeran zakonitom cilju istraživanja nekoliko pokušaja ubojstva te je stoga bio nužan u demokratskom društvu. Sud je zaključio da nije prekršen članak 8. Konvencije.

Oblik prikazivanja podataka

Oblik u kojem se osobni podaci pohranjuju ili koriste nije relevantan za primjenjivost zakonodavstva o zaštiti podataka. Pismena ili usmena komunikacija može sadržavati osobne podatke kao i slike,[63] uključujući snimku[64] ili zvuk televizije zatvorenog kruga (CCTV).[65] Elektronički snimljena informacija, kao i papirnata informacija, također mogu biti osobni podaci; čak i stanični uzorci ljudskog tkiva mogu biti osobni podaci jer reproduciraju DNK pojedinca.

2.1.2. Posebne kategorije osobnih podataka

Unutar prava Europske unije kao i **unutar prava Vijeća Europe** postoje posebne kategorije osobnih podataka koji zbog svoje prirode prilikom obrade mogu predstavljati rizik za osobe čiji se podaci obrađuju te ih stoga treba dodatno zaštititi. Obradu takvih posebnih kategorija osobnih podataka („osjetljivi podaci") iz tog razloga valja dopustiti samo uz poduzimanje konkretnih mjera zaštite.

62 ECtHR, *Uzun protiv Njemačke*, br. 35623/05, 2. rujna 2010.

63 ECtHR, *Von Hannover protiv Njemačke*, br. 59320/00, 24. lipnja 2004.; ECtHR, *Sciacca protiv Italije*, br. 50774/99, 11. siječnja 2005.

64 ECtHR, *Peck protiv Ujedinjene Kraljevine*, br. 44647/98, 28. siječnja 2003.; ECtHR, *Köpke protiv Njemačke*, br. 420/07, 5. listopada 2010.

65 Direktiva o zaštiti podataka, uvodne izjave 16. i 17.; ECtHR, *P.G. i J.H. protiv Ujedinjene Kraljevine*, br. 44787/98, 25. rujna 2001., st. 59. i 60.; ECtHR, *Wisse protiv Francuske*, br. 71611/01, 20. prosinca 2005.

Prilikom definiranja osjetljivih podataka i Konvencija br. 108 (članak 6.) i Direktiva o zaštiti podataka (članak 8.) navode sljedeće kategorije:

- osobni podaci kojima se otkriva rasno ili etničko podrijetlo
- osobni podaci kojima se otkrivaju politička mišljenja, vjerska ili druga uvjerenja
- osobni podaci u vezi sa zdravljem ili spolnim životom.

> Primjer: U predmetu *Bodil Lindqvist*,[66] Sud Europske unije izjavio je da „pozivanje na činjenicu da je osoba ozlijedila stopalo, a zaposlena je na nepuno radno vrijeme iz medicinskih razloga predstavlja osobne podatke koji se tiču zdravlja u smislu članka 8. stavka 1. Direktive 95/46."

Direktiva o zaštiti podataka nadalje navodi „članstvo u sindikatu" kao osjetljiv podatak, jer ta informacija može biti očit pokazatelj političkog uvjerenja ili pripadnosti.

Prema Konvenciji br. 108 i osobni podaci vezani uz krivične presude smatraju se osjetljivim podacima.

Članak 8. stavak 7. Direktive o zaštiti podataka države članice ovlašćuje da „utvrde uvjete pod kojima se obrađuje nacionalni identifikacijski broj ili bilo koji drugi način identifikacije za opću uporabu."

2.1.3. Anonimizirani i pseudonimizirani podaci

Sukladno načelu ograničenog zadržavanja podataka sadržanom u Direktivi o zaštiti podataka te Konvenciji br. 108 (o kojem se detaljnije raspravlja u poglavlju 3.), podaci se čuvaju „u obliku koji omogućava identifikaciju osoba čiji se podaci obrađuju samo tijekom razdoblja potrebnog u svrhe zbog kojih se podaci prikupljaju ili zbog kojih se dalje obrađuju."[67] Sukladno tome, kada zastare i više ne služe prvobitnoj svrsi, podaci bi se trebali anonimizirati želi li ih nadzornik pohraniti.

66 CJEU, C-101/01, *Bodil Lindqvist*, 6. studenoga . 51.

67 Direktiva o zaštiti podataka, čl. 6. st. 1. točka (e); i Konvencija br. 108, čl. 5. točka (e).

Anonimizirani podaci

Podaci su anonimizirani ako su svi elementi identifikacije uklonjeni iz zbirke osobnih podataka. U njima ne smije ostati nijedan element koji bi mogao poslužiti da se, uz razuman trud, dotična(e) osoba(e) ponovno identificira(ju).[68] Kada se podaci uspješno anonimiziraju, to više nisu osobni podaci.

Ako osobni podaci više ne služe prvobitnoj svrsi, ali se moraju čuvati u personaliziranom obliku u povijesne, statističke ili znanstvene svrhe, Direktiva o zaštiti podataka i Konvencija br. 108 to omogućuju pod uvjetom da se poduzmu odgovarajuće mjere zaštite.[69]

Pseudonimizirani podaci

Osobne informacije sadrže identifikatore poput imena, datuma rođenja, spola i adrese. Kada se osobne informacije pseudonimiziraju, identifikatori se zamjenjuju pseudonimom. Pseudonimizacija se postiže, na primjer, šifriranjem identifikatora u osobnim podacima.

Pseudonimizirani podaci ne spominju se izričito u pravnim definicijama Konvencije br. 108 ili Direktive o zaštiti podataka. Unatoč tome, eksplanatorno izvješće uz Konvenciju br. 108 u članku 42. navodi "[ ] zahtjev [...] u vezi s vremenskim rokovima pohrane podataka u obliku koji je povezan s imenom ne znači da se podaci nakon izvjesnog vremena trebaju neopozivo odvojiti od imena osobe na koju se odnose, već samo da ne bi trebalo biti moguće smjesta povezati podatke i identifikatore". To se može postići pseudonimizacijom podataka. Svi oni koji nemaju ključ za dešifriranje mogu otežano identificirati pseudonimizirane podatke. Ipak, i dalje postoji poveznica s identitetom u obliku pseudonima uz ključ za dešifriranje. Oni koji su ovlašteni koristiti takav ključ mogu ponovno, na jednostavniji način, identificirati osobu. Posebno valja spriječiti uporabu ključeva za dešifriranje od strane neovlaštenih osoba.

Kako je pseudonimizacija podataka jedan od najvažnijih načina za opsežnu zaštitu podataka, kada se nije moguće u cijelosti suzdržati od uporabe osobnih podataka, valja detaljnije obrazložiti logiku i učinak uporabe.

68 *Ibid.*, uvodna izjava 26.

69 *Ibid.*, čl. 6. stavak 1. točka (e); i Konvencija br. 108, članak 5. točka (e).

Primjer: Rečenica „Charles Spencer, rođen 3. travnja 1967., otac je četvero djece, dvaju dječaka i dviju djevojčica” može se primjerice pseudonimizirati na sljedeći način:

„C.S. 1967. otac je četvero djece, dvaju dječaka i dviju djevojčica” ili

„324. otac je četvero djece, dvaju dječaka i dviju djevojčica” ili

„YESz320l otac je četvero djece, dvaju dječaka i dviju djevojčica”.

Korisnici koji pristupe takvim pseudonimiziranim podacima obično neće moći identificirati „Charlesa Spencera, rođenog 3. travnja na temelju pseudonima „324” ili „YESz3201”. Zato su pseudonimizirani podaci češće zaštićeni od zloporabe.

No prvi je navedeni primjer manje siguran. Ako se rečenica „C.S. 1967. otac je četvero djece, dvaju dječaka i dviju djevojčica” koristi u malenom selu u kojem Charles Spencer živi, moglo bi ga se lako prepoznati. Metoda pseudonimizacije utječe na učinkovitost zaštite podataka.

Osobni podaci šifriranih identifikatora u mnogim se slučajevima koriste kako bi se zatajio identitet osoba. To je osobito korisno kada nadzornici moraju osigurati da se bave istim osobama čiji se podaci obrađuju, no ne zahtijevaju, ili ne bi smjeli dobiti, stvarni identitet osoba. To se događa kada na primjer istraživač istražuje tijek bolesti pacijenata čiji je identitet poznat samo bolnici u kojoj se pacijent liječi i koja istraživaču dostavlja pseudonimizirane povijesti slučajeva. Pseudonimizacija je dakle snažna karika u lancu tehnologije za zaštitu privatnosti. Ona može biti važan element u provedbi ugrađene privatnosti. To znači da je zaštita podataka ugrađena u tkivo naprednih sustava obrade podataka.

2.2. Obrada podataka

Ključne točke

- Pojam „obrada” u prvom se redu odnosi na automatsku obradu.
- Unutar prava Europske unije, „obrada” se odnosi i na ručnu obradu u strukturiranim sustavima arhiviranja.

- Unutar prava Vijeća Europe, značenje „obrade" može se proširiti u okviru nacionalnog zakonodavstva kako bi obuhvatilo ručnu obradu.

Zaštita podataka prema Konvenciji br. 108 i Direktivi o zaštiti podataka prvenstveno je usredotočena na automatsku obradu podataka.

Unutar **prava Vijeća Europe,** u definiciji automatske obrade, prepoznato je da među pojedinim automatskim radnjama mogu biti potrebne određene faze ručne uporabe osobnih podataka. Slično je i unutar **prava Europske unije**, koje automatsku obradu podataka definira kao „radnje koje se vrše na osobnim podacima, u cijelosti ili djelomično automatskim putem".[70]

Primjer: U predmetu *Bodil Lindqvist*,[71] Sud Europske unije smatrao je da se:

„upućivanje na različite osobe na internetskoj stranici te njihovo identificiranje imenom ili na drugi način, primjerice navođenje njihova telefonskog broja ili informacija u vezi s njihovim radnim uvjetima ili hobijima, smatra „osobnim podacima koji se u cijelosti ili djelomično obrađuju automatskim putem" u smislu članka 3. stavka 1. Direktive 95/46."

Ručna obrada podataka također zahtijeva zaštitu podataka.

Zaštita podataka **unutar prava Europske unije** ni na koji način nije ograničena na automatsku obradu podataka. Isto tako, unutar prava Europske unije, zaštita podataka primjenjuje se na obradu osobnih podataka u ručnim sustavima arhiviranja, tj. posebno strukturiranoj papirnoj datoteci.[72] Razlog ovakvog proširenja zaštite podataka je što:

- papirne datoteke mogu biti strukturirane tako da omogućuju brzo i jednostavno pronalaženje informacija

- se pohranom osobnih podataka u strukturiranim papirnim datotekama lakše zaobilaze zakonski propisana ograničenja automatske obrade podataka.[73]

70 Konvencija br. 108, čl. 2. točka (c); i Direktiva o zaštiti podataka, čl. 2. točka (b) i čl. 3. stavak 1.

71 CJEU, C-101/01, *Bodil Lindqvist*, 6. studenoga . 27.

72 Direktiva o zaštiti podataka, čl. . 1.

73 *Ibid*., uvodna izjava 27.

Unutar prava Vijeća Europe, Konvencija br. 108 prvenstveno regulira obradu podataka u automatiziranoj bazi podataka.[74] No ona također pruža mogućnost proširenja zaštite na ručnu obradu u okviru nacionalnog zakonodavstva. Mnoge su stranke Konvencije br. 108 iskoristile tu mogućnost i u tu svrhu dale izjavu glavnom tajniku Vijeća Europe.[75] Proširenje zaštite podataka iz takve izjave mora se odnositi na sve ručne obrade podataka i ne može se ograničiti na obradu u ručnim sustavima arhiviranja.[76]

Što se tiče prirode uključenih obrada, i **pravo Europske unije i pravo Vijeća Europe** uključuju pojam obrade: „obrada osobnih podataka" [...] znači bilo koji postupak [...] kao što je prikupljanje, snimanje, organiziranje, pohrana, prilagođavanje ili mijenjanje, vraćanje, obavljanje uvida, uporaba, otkrivanje prijenosom i širenjem, ili stavljanje na raspolaganje drugim načinom, poravnavanje ili kombiniranje, blokiranje, brisanje ili uništavanje"[77] koji se provodi na osobnim podacima. Pojam „obrada" uključuje i one postupke u kojima odgovornost za podatke prelazi s jednog nadzornika na drugog.

Primjer: Poslodavci prikupljaju i obrađuju podatke o svojim zaposlenicima, uključujući informacije o njihovim plaćama. Pravna osnova za zakonitost tog čina jest ugovor o radu.

Poslodavci podatke o plaćama zaposlenika prosljeđuju poreznim tijelima. Takvo se prosljeđivanje podataka također smatra „obradom" u smislu značenja te riječi u Konvenciji br. 108 i direktivi. No, pravna osnova za zakonitost takvog otkrivanja podataka nije ugovor o radu. Mora postojati dodatna pravna osnova za postupke obrade koji podrazumijevaju prijenos podataka o plaćama na relaciji poslodavac – porezno tijelo. Ta je pravna osnova obično sadržana u odredbama nacionalnih poreznih zakona. Bez takvih bi se odredbi prijenos podataka smatrao nezakonitom obradom.

74 Konvencija br. 108, čl 2. točka (b).

75 Vidjeti izjave dane sukladno Konvenciji br. 108, čl. 3. stavak 2. točka (c).

76 Vidjeti izjave dane sukladno Konvenciji br. 108, čl. 3. stavak 2.

77 Direktiva o zaštiti podataka, čl. 2. točka (b). Pogledati i Konvenciju br. 108, čl. 2 točka (c).

2.3. Korisnici osobnih podataka

Ključne točke

- Onaj koji odluči obrađivati osobne podatke drugih, sukladno zakonodavstvu o zaštiti podataka, naziva se „nadzornik"; ako nekoliko ljudi zajednički donosi tu odluku, oni mogu biti „zajednički nadzornici".
- „Obrađivač" je pravno zaseban subjekt koji obrađuje osobne podatke u ime nadzornika.
- Obrađivač postaje nadzornik ako koristi podatke u vlastite svrhe, a ne prati upute nadzornika.
- Svatko tko primi podatke od nadzornika je „primatelj".
- „Treća stranka" je fizička ili pravna osoba koja ne radi po uputama nadzornika (i nije osoba čiji se podaci obrađuju).
- „Primatelj treće stranke" je osoba ili subjekt koja je pravno odvojena od nadzornika, ali prima osobne podatke od nadzornika.

2.3.1. Nadzornici i obrađivači

Najvažnija je posljedica obnašanja funkcije nadzornika ili obrađivača pravna odgovornost za ispunjavanje odgovarajućih obveza koje proizlaze iz zakonodavstva o zaštiti podataka. Stoga samo oni koji se mogu smatrati odgovornima sukladno primjenjivom pravu mogu vršiti tu funkciju. U privatnom je sektoru to obično fizička ili pravna osoba; a u javnom sektoru, nadležno tijelo. Drugi subjekti, poput tijela ili institucija bez pravne osobnosti, mogu biti nadzornici ili obrađivači samo ako tako nalažu posebni propisi.

Primjer: Kad marketinški odjel društva Sunshine planira obrađivati podatke u svrhe istraživanja tržišta, onda je nadzornik društvo Sunshine, a ne marketinški odjel. Marketinški odjel ne može biti nadzornik jer nema zasebnu pravnu osobnost.

Kada se radi o grupacijama, matično društvo i sva ovisna društva, kao zasebne pravne osobe, smatraju se zasebnim nadzornicima ili obrađivačima. Posljedica je takvog pravno zasebnog statusa da se za prijenos podataka među članovima grupacije zahtijeva posebna pravna osnova. Ne postoji povlastica koja bi omogućila

razmjenu osobnih podataka kao takvih među zasebnim pravnim subjektima unutar grupacije.

U ovom kontekstu valja spomenuti ulogu fizičkih osoba. **Unutar prava Europske unije**, kad fizičke osobe obrađuju podatke o drugima tijekom aktivnosti isključivo osobne ili domaće naravi, ne primjenjuju se odredbe Direktive o zaštiti podataka; one se ne smatraju nazdornicima.[78]

Unatoč tome, sudska praksa nalaže da se zakonodavstvo o zaštiti podataka ipak primjenjuje kada fizička osoba koristeći internet objavi podatke o drugima.

Primjer: Sud Europske unije u predmetu *Bodil Lindqvist*[79] smatrao je da:

„upućivanje na različite osobe na internetskoj stranici te njihovo identificiranje imenom ili na drugi način [...] smatra se „osobnim podacima koji se u cijelosti ili djelomično obrađuju automatskim putem" u smislu članka 3. stavka 1. Direktive 95/46."[80]

Takva obrada osobnih podataka ne spada u aktivnosti isključivo osobne ili domaće naravi koje su izvan područja primjene Direktive o zaštiti podataka, jer se takva iznimka „mora [...] tumačiti kao da se odnosi samo na aktivnosti koje se vrše u okviru privatnog ili obiteljskog života pojedinaca, što očito nije slučaj s obradom osobnih podataka koja podrazumijeva objavu na internetu te stavljanje na raspolaganje podataka neograničenom broju ljudi ."[81]

Nadzornik

Unutar prava Europske unije nadzornik se definira kao onaj koji „sam ili zajedno s drugima utvrđuje svrhu i načine obrade osobnih podataka".[82] Odluka je nadzornika zašto se i kako podaci obrađuju. **Unutar prava Vijeća Europe**, u definiciji „nadzornika" dodatno se navodi da nadzornik odlučuje o tome koje će se kategorije osobnih podataka pohraniti.[83]

78 Direktiva o zaštiti podataka, uvodna izjava 12. i čl. 3. stavak 2. zadnja alineja.

79 CJEU, C-101/01, *Bodil Lindqvist*, 6. studenoga 2003.

80 *Ibid.*, st. 27.

81 *Ibid.*, st. 47.

82 Direktiva o zaštiti podataka, čl. 2. točka (d).

83 Konvencija br. 108, čl. 2. točka (d).

U definiciji nadzornika iz Konvencije br. 108 spominje se još jedan aspekt nadzora koji valja razmotriti. Ta se definicija naime odnosi na pitanje tko može zakonito obrađivati određene podatke u određene svrhe. No, kada su posrijedi navodno nezakoniti postupci obrade i treba pronaći odgovornog nadzornika, smatra se da je nadzornik osoba ili subjekt, kao što je društvo ili nadležno tijelo, koja je odlučila da podatke treba obraditi, neovisno o tome je li bila pravno ovlaštena takvo što odlučiti ili ne.[84] Zahtjev za brisanje stoga uvijek valja uputiti „činjeničnom" nadzorniku.

Zajednički nadzor

Definicija „nadzornika" u Direktivi o zaštiti podataka navodi da može biti više pravno zasebnih subjekata koji zajednički ili s drugima vrše funkciju nadzornika. To znači da zajedno odlučuju o obradi podataka u zajedničke svrhe.[85] To je pravno moguće, no samo u slučajevima kada posebna pravna osnova omogućuje zajedničku obradu podataka u zajedničke svrhe.

Primjer: Opći primjer zajedničkog nadzora je baza podataka koju za svoje klijente zajednički vodi nekoliko kreditnih institucija. Kada podnositelj zatraži kredit od banke koja je jedna od zajedničkih nadzornika, banke provjeravaju bazu podataka radi lakšeg donošenja odluke na temelju primljenih informacija o kreditnoj sposobnosti podnositelja zahtjeva.

Propisi ne navode izričito zahtijeva li zajednički nadzor da zajednička svrha bude ista za svakog nadzornika ili je li dovoljno da se njihove svrhe tek djelomično preklapaju. Ipak, na europskoj razini još nema sudske prakse niti su jasne posljedice koje se tiču odgovornosti. Radna skupina iz članka 29. zagovara šire tumačenje pojma zajedničkog nadzora u cilju fleksibilnosti kojom bi se odgovorilo na sve složeniju trenutnu situaciju po pitanju obrade podataka.[86] Slučaj u koji je bilo uključeno Društvo za svjetsku međubankovnu financijsku telekomunikaciju (SWIFT) ilustrira stajalište Radne skupine.

Primjer: U takozvanom slučaju SWIFT, europske bankovne institucije angažirale su SWIFT, prvobitno kao obrađivača, za operacije prijenosa podataka tijekom

84 Vidjeti i *Mišljenje 1/2010* Radne skupine iz članka 29. (2010) o *pojmovima „voditelj zbirke osobnih podataka" i „obrađivač"*, WP 169, Bruxelles, 16. veljače 2010., str. 15.

85 Direktiva o zaštiti podataka, čl. 2. točka (d).

86 Vidjeti i *Mišljenje 1/2010* Radne skupine iz članka 29. (2010.) o *pojmovima „voditelj zbirke osobnih podataka" i „obrađivač"*, WP 169, Bruxelles, 16. veljače 2010., st. 19.

bankovnih transakcija. SWIFT je te podatke o bankovnim transakcijama, pohranjene u računalnom uslužnom centru SAD-a, otkrio Odjelu državne riznice SAD-a iako mu to nisu izričito naložile europske bankarske institucije koje su SWIFT angažirale. Prilikom procjene zakonitosti ove situacije, Radna skupina iz članka 29. zaključila je da se na europske bankarske institucije koje su angažirale SWIFT, kao i na sam SWIFT, treba gledati kao na zajedničke nadzornike koji europskim klijentima odgovaraju za otkrivanje njihovih podataka nadležnim tijelima SAD-a.[87] Odlučujući otkriti podatke SWIFT je nezakonito preuzeo ulogu nadzornika; bankarske institucije očito nisu ispunile svoju obvezu nadgledanja svojeg obrađivača te ih se stoga nije moglo u cijelosti osloboditi odgovornosti koju su imale kao nadzornici. Ishod je ove situacije zajednički nadzor.

Obrađivač

Obrađivač se **unutar prava Europske unije** definira kao osoba koja obrađuje osobne podatke u ime nadzornika.[88] Aktivnosti povjerene obrađivaču mogu se ograničiti na vrlo konkretnu zadaću ili kontekst ili mogu biti prilično općenite i sveobuhvatne.

Unutar prava Vijeća Europe, značenje pojma obrađivača isto je kao i unutar prava Europske unije.

Osim što obrađuju podatke za druge, obrađivači su također i nadzornici s obzirom na obradu podataka koju vrše u vlastite svrhe, npr. upravljanje vlastitim zaposlenicima, plaćama i računima.

Primjeri: Društvo Everready specijalizirano je za obradu podataka za vođenje podataka o ljudskim potencijalima za druga društva. U toj je funkciji Everready obrađivač.

No kada društvo Everready obrađuje podatke svojih zaposlenika, ono je nadzornik za postupke obrade podataka jer time ispunjava svoju obvezu kao poslodavac.

87 Radna skupina iz članka 29. (2006.), *Mišljenje 10/2006 o obradi osobnih podataka od strane Društva za svjetsku međubankovnu financijsku telekomunikaciju (SWIFT),* WP 128, Bruxelles, 22. studenoga 2006.

88 Direktiva o zaštiti podataka, čl. 2. točka (e).

Odnos između nadzornika i obrađivača

Kao što je rečeno, nadzornik je definiran kao onaj koji utvrđuje svrhu i načine obrade.

> Primjer: Direktor društva Sunshine odlučio je da društvo Moonlight, specijalizirano za marketinške analize, provede marketinšku analizu podataka o kupcima društva Sunshine. Iako je zadaća utvrđivanja načina obrade povjerena društvu Moonlight, društvo Sunshine je nadzornik, a društvo Moonlight samo obrađivač, jer, prema ugovoru, Moonlight može koristiti podatke o kupcima društva Sunshine samo u svrhe koje utvrdi Sunshine.

Ako se ovlast utvrđivanja načina obrade povjeri obrađivaču, nadzornik svejedno mora imati utjecaj na odluke obrađivača u pogledu načina obrade. Sveukupna odgovornost ostaje na strani nadzornika, koji mora nadgledati obrađivače kako bi osigurao da su njihove odluke u skladu sa zakonodavstvom o zaštiti podataka. Iz tog bi se razloga ugovor kojim se nadzorniku brani uplitanje u odluke obrađivača vjerojatno tumačio na način da iz njega proizlazi zajednički nadzor koji podrazumijeva da obje stranke dijele pravu odgovornost nadzornika.

Nadalje, u slučaju da obrađivač ne bi poštivao ograničenja uporabe podataka na način koji propiše nadzornik, obrađivač postao bi nadzornik bar u opsegu kršenja uputa nadzornika. U tom će slučaju obrađivač najvjerojatnije postati nadzornik koji djeluje nezakonito, a prvobitni nadzornik morat će objasniti kako je obrađivač mogao prekršiti svoj mandat. Radna skupina iz članka 29. zaista često pretpostavlja da su takvi slučajevi stvar zajedničkog nadzora jer je to u najboljem interesu zaštite osoba čiji se podaci obrađuju.[89] Važna bi posljedica zajedničkog nadzora trebala biti skupna i solidarna odgovornost za štetu koja bi osobama čiji se podaci obrađuju omogućila veći broj pravnih lijekova.

Pitanje o podjeli odgovornosti može se javiti i kada je nadzornik malo poduzeće, a obrađivač velika korporacija koja može diktirati uvjete usluga koje pruža. U takvim okolnostima Radna skupina iz članka 29. smatra da se standard odgovornosti ne

89 Radna skupina iz članka 29. (2010.), *Mišljenje 1/2010 o pojmovima „nadzornik" i „obrađivač"*, WP 169, Bruxelles, 16. veljače 2010., st. 25; i Radna skupina iz članka 29. (2006.), *Mišljenje 10/2006 o obradi osobnih podataka od strane Društva za svjetsku međubankovnu financijsku telekomunikaciju (SWIFT)*, WP 128, Bruxelles, 22. studenoga 2006.

smije snižavati zbog ekonomske nejednakosti i da se mora zadržati shvaćanje pojma nadzornika.[90]

Radi jasnoće i transparentnosti, detalje odnosa nadzornika i obrađivača treba urediti pismenim ugovorom.[91] U suprotnom se krši obveza nadzornika u pogledu predočavanja pismene dokumentacije o uzajamnim odgovornostima, što može dovesti do kazni.[92]

Obrađivači mogu prepustiti određene zadaće podizvođačima obrade. To je zakonski dopušteno, a konkretno ovisi o ugovornim odredbama između nadzornika i obrađivača, uključujući činjenicu je li ovlaštenje nadzornika nužno baš u svakom slučaju ili je dovoljna samo obavijest.

Unutar prava Vijeća Europe, u cijelosti je primjenjivo tumačenje pojmova nadzornika i obrađivača, kako je gore opisano, na što ukazuju preporuke donesene sukladno Konvenciji br. 108.[93]

2.3.2. Primatelji i treće stranke

Razlika između ove dvije kategorije osoba ili subjekata, uvedene Direktivom o zaštiti podataka, uglavnom se odnosi na odnos koji imaju s nadzornikom te posljedično na ovlaštenje za pristup osobnim podacima navedenoga nadzornika.

„Treća stranka" pravno se razlikuje od nadzornika pa će za otkrivanje podataka trećoj stranki uvijek biti potrebna konkretna pravna osnova. Prema članku 2. točki (f) Direktive o zaštiti podataka, treća stranka je „bilo koja fizička ili pravna osoba, javno tijelo, agencija ili bilo koje drugo tijelo osim osobe čiji se podaci obrađuju, nadzornika, obrađivača i osoba koje su na temelju izravne ovlasti nadzornika ili obrađivača ovlaštene obrađivati podatke". To znači da će osobe koje rade za organizaciju koja se pravnim oblikom razlikuje od nadzornika – čak i ako pripada istoj grupaciji ili holdingu – biti „treća stranka" (ili će joj pripadati). S druge strane, poslovnice banke koje

90 Vidjeti i *Mišljenje 1/2010* Radne skupine iz članka 29. (2010) o *pojmovima „nadzornik" i „obrađivač"*, WP 169, Bruxelles, 16. veljače 2010., st. 26.

91 Direktiva o zaštiti podataka, čl. . 3. i 4.

92 Vidjeti i *Mišljenje 1/2010* Radne skupine iz članka 29. (2010) o *pojmovima „nadzornik" i „obrađivač"*, WP 169, Bruxelles, 16. veljače 2010., str. 27.

93 Vidjeti primjerice Preporuku o profiliranju, čl. 1.

obrađuju račune klijenata pod izravnom ovlasti svojih sjedišta neće se smatrati „trećim strankama".[94]

„Primatelj" je širi pojam od „treće stranke". U smislu članka 2. točke (g) Direktive o zaštiti podataka, primatelj je „fizička ili pravna osoba, javno tijelo, agencija ili bilo koje drugo tijelo kojem se podaci otkrivaju, bilo da je treća stranka ili ne". Primatelj može biti ili osoba izvan tijela nadzornika ili obrađivača – u tom je slučaju to treća stranka – ili netko unutar tijela nadzornika ili obrađivača, kao što je zaposlenik ili drugi odjel unutar istog društva ili tijela.

Razlika između primatelja i trećih stranki važna je samo zbog uvjeta za zakonito otkrivanje podataka. Zaposlenici nadzornika ili obrađivača bez dodatnih pravnih zahtjeva mogu biti primatelji osobnih podataka ako su uključeni u postupke obrade nadzornika ili obrađivača. S druge strane, s obzirom na to da je treća stranka pravno zaseban subjekt od nadzornika ili obrađivača, ona nije ovlaštena koristiti osobne podatke koje obradi nadzornik, osim ako za to u konkretnom slučaju postoje konkretne pravne osnove. „Primateljima trećim strankama" podataka stoga će uvijek trebati pravna osnova za zakonito primanje osobnih podataka.

Primjer: Zaposlenik obrađivača koji koristi osobne podatke u okviru zadaća koje mu je povjerio poslodavac je primatelj podataka, ali nije treća stranka jer koristi podatke u ime i prema uputama obrađivača.

No, odluči li isti taj zaposlenik u vlastite svrhe iskoristiti podatke, kojima može pristupiti kao zaposlenik obrađivača, i proda ih drugom društvu, tada je zaposlenik djelovao kao treća stranka. U tom slučaju on više ne slijedi upute obrađivača (poslodavca). Zaposleniku bi, kao trećoj stranki, trebala pravna osnova za stjecanje i prodaju podataka. U ovom slučaju zaposlenik zasigurno nema takvu pravnu osnovu pa su takve radnje nezakonite.

94 *Mišljenje 1/2010* Radne skupine iz članka 29. (2010.) *o pojmovima „nadzornik" i „obrađivač"*, WP 169, Bruxelles, 16. veljače 2010., str. 31.

2.4. Suglasnost

Ključne točke

- Kao pravna osnova za obradu osobnih podataka, suglasnost mora biti dobrovoljno dana, posebna i utemeljena na informacijama.
- Isto tako, dana suglasnost mora biti nedvosmislena. Suglasnost se može dati izričito ili implicitno i to na način koji ne dovodi u sumnju da je osoba čiji se podaci obrađuju suglasna s obradom svojih podataka.
- Za obradu osjetljivih podataka na temelju suglasnosti potrebna je izričita suglasnost.
- Suglasnost se može povući u svakom trenutku.

Suglasnost znači „svaka dobrovoljno dana, posebna i informirana izjava volje."[95] U brojnim je slučajevima ona pravna osnova za zakonitu obradu podataka (vidjeti odjeljak 4.1).

2.4.1. Elementi valjane suglasnosti

Sukladno **pravu Europske unije** tri su elementa preduvjeti da bi suglasnost bila valjana. Njima se jamči da su osobe čiji se podaci obrađuju zaista pristale na uporabu svojih podataka:

- osoba čiji se podaci obrađuju ne smije biti pod pritiskom prilikom davanja suglasnosti
- osoba čiji se podaci obrađuju mora biti propisno informirana o predmetu i posljedicama davanja suglasnosti
- područje primjene suglasnosti mora biti konkretno u prihvatljivoj mjeri.

Suglasnost će biti valjana u smislu zakonodavstva o zaštiti podataka samo ako su ispunjeni svi navedeni preduvjeti.

Konvencija br. 108 ne sadrži definiciju suglasnosti; to je prepušteno nacionalnim zakonodavstvima. Ipak, **unutar prava Vijeća Europe**, elementi valjane suglasnosti

95 Direktiva o zaštiti podataka, čl. 2. točka (h).

odgovaraju onima koji su prethodno spomenuti, kako stoji u preporukama koje su izrađene sukladno Konvenciji br. 108.[96] Zahtjevi za suglasnost isti su kao i za izjavu o namjeri iz europskog građanskog prava.

Dodatni zahtjevi za valjanu suglasnost unutar građanskog prava, kao što je pravna sposobnost, također se primjenjuju i u kontekstu zaštite podataka, jer su takvi zahtjevi temeljni pravni preduvjeti. Nevaljana suglasnost osoba bez pravne sposobnosti podrazumijeva nedostatak pravne osnove za obradu podataka o takvim osobama.

Suglasnost se može dati izričito[97] ili neizričito. Izričita suglasnost ne dovodi u sumnju namjere osobe čiji se podaci obrađuju i može se dati usmeno ili pismeno; neizričita suglasnost utvrđuje se na temelju okolnosti. Svaka se suglasnost mora dati nedvosmisleno.[98] To znači da ne smije izazivati opravdanu sumnju da je osoba čiji se podaci obrađuju željela izraziti svoje slaganje s obradom svojih podataka. Nečija puka neaktivnost tako ne znači da je dotični dao nedvosmislenu suglasnost. Kada su podaci koji se obrađuju osjetljive prirode, obvezna je izričita suglasnost koja mora biti nedvosmislena.

Dobrovoljna suglasnost

Postojanje dobrovoljne suglasnosti valjano je samo „ako osoba čiji se podaci obrađuju može zaista birati bez opasnosti od obmane, zastrašivanja, prisile ili bitno negativnih posljedica ako uskrati suglasnost".[99]

Primjer: U mnogim zračnim lukama putnici moraju proći kroz skenere tijela kako bi pristupili ukrcaju u zrakoplov.[100] Budući da se tijekom skeniranja obrađuju podaci o putnicima, obrada mora biti u skladu s jednom od pravnih osnova iz članka 7. Direktive o zaštiti podataka (vidi odjeljak 4.1.1). Prolazak kroz skenere tijela ponekad se putnicima predstavlja kao opcija, pri čemu se podrazumijeva da suglasnost može opravdati obradu. No putnici se mogu pribojavati da će njihovo odbijanje skeniranja tijela biti sumnjivo ili povlačiti dodatne kontrole poput

96 Vidjeti primjerice Konvenciju br. 108, Preporuku o statističkim podacima, točku 6.

97 Direktiva o zaštiti podataka, čl. . 2.

98 *Ibid.*, *čl.* 7. pod (a) i čl. 26. stavak 1.

99 Vidi i *Mišljenje 15/2011* Radne skupine iz članka 29. (2011.) *o pojmu suglasnosti*, WP 187, Bruxelles, 13. srpnja 2011., str. 12.

100 Ovaj je primjer uzet iz *Ibid.*, str. 15.

pretraživanja tijela. Mnogi putnici pristaju na skeniranje jer tako izbjegavaju potencijalne probleme ili kašnjenja. Takva suglasnost ne smatra se dobrovoljnom u dovoljnoj mjeri.

Stoga se solidna legitimna osnova može pronaći samo u zakonodavnom aktu iz kojeg, na temelju članka 7. točke (e) Direktive o zaštiti podataka, proizlazi obveza suradnje putnika radi prevladavajućeg javnog interesa. No, zakonodavstvo ipak može ostaviti izbor između skeniranja i pretraživanja, ali samo kao dio dodatnih mjera granične kontrole koje su nužne u određenim okolnostima. Tako su glasile dvije uredbe Europske komisije iz 2011. koje su se ticale zaštitnih skenera.[101]

Dobrovoljni pristanak također može biti ugrožen u situacijama podređenosti, tj. kada postoji značajna ekonomska ili druga neravnoteža između nadzornika koji osigurava suglasnost i osobe čiji se podaci obrađuju koja daje suglasnost.[102]

Primjer: Velika kompanija planira izraditi registar s imenima svih zaposlenika, njihovim funkcijama u kompaniji i poslovnim adresama, i to isključivo u svrhe unapređenja unutarnje komunikacije kompanije. Voditelj kadrovske službe predlaže da se u registar uz svako ime zaposlenika doda i slika kako bi se, primjerice, kolege lakše međusobno prepoznali na sastancima. Predstavnici zaposlenika traže da se to učini isključivo ako na to pristane svaki zaposlenik posebno.

U ovoj se situaciji suglasnost zaposlenika treba priznati kao pravna osnova za obradu fotografija u registru jer je jasno da objava fotografije u registru sama po sebi nema negativne posljedice te je isto tako vjerojatno da se zaposlenik neće suočiti s negativnim radnjama poslodavca u slučaju da ne pristane na objavu fotografije u registru.

101 Uredba komisije (EU) br. 1141/2011. od 10. studenoga 2011. o izmjeni Uredbe (EZ) br. 272/2009. o dopuni zajedničkih osnovnih standarda o zaštiti civilnog zračnog prometa u vezi s upotrebom zaštitnih skenera u zračnim lukama EU-a, SL L 2011 L 293, i Provedbena uredba Komisije (EU) br. 1147/2011 od 11. studenoga 2011. o izmjeni Uredbe (EU) br. 185/2010 o provedbi zajedničkih osnovnih standarda o zaštiti civilnog zračnog prometa u vezi s upotrebom zaštitnih skenera u zračnim lukama EU-a, SL L 2011 L 294.

102 Vidjeti i *Mišljenje 8/2001* Radne skupine iz članka 29. (2001.) *o obradi osobnih podataka u kontekstu zapošljavanja*, WP 48, Bruxelles, 13. rujna 2001.; i Radna skupina iz članka 29. (2005.), *Radni dokument o zajedničkom tumačenju članka 26. stavka 1. Direktive 95/46/EZ od 24. listopada 1995.*, WP 114, Bruxelles, 25. studenoga 2005.

No to ne znači da suglasnost nikada ne može biti valjana u okolnostima u kojima bi uskrata suglasnosti imala negativne posljedice. Ako primjerice nesuglasnost za preuzimanje kartice nekog supermarketa za ishod ima samo neostvarivanje popusta na cijene određenih artikala, suglasnost je ipak valjana pravna osnova za obradu osobnih podataka onih kupaca koji su pristali na karticu. Između društva i kupca u tom slučaju nema podređenosti, a posljedice uskrate suglasnosti nisu dovoljno ozbiljne da bi spriječile slobodan izbor osobe čiji se podaci obrađuju.

S druge strane, uvijek kada se dovoljno bitni proizvodi ili usluge mogu dobiti samo i isključivo ako se određeni osobni podaci otkriju trećim stranama, suglasnost osobe čiji se podaci obrađuju na otkrivanje vlastitih podataka obično se ne može smatrati slobodnom odlukom te stoga nije valjana sukladno zakonodavstvu o zaštiti podataka.

Primjer: Ako putnici zračne kompanije pristanu da ona prenese takozvane evidencije imena putnika (PNR), odnosno podatke o njihovu identitetu, prehrambenim navikama ili zdravstvenim problemima nadležnim tijelima za imigraciju određene strane zemlje, to se ne može smatrati valjanom suglasnošću sukladno zakonodavstvu o zaštiti podataka jer putnici nemaju izbora ako žele posjetiti tu zemlju. Da bi se takvi podaci zakonito prenijeli, potrebna je druga pravna osnova osim suglasnosti, a to najvjerojatnije poseban zakon.

Suglasnost utemeljena na informacijama

Osoba čiji se podaci obrađuju mora imati dovoljno informacija prije donošenja odluke. Jesu li pružene informacije dostatne ili ne može se utvrditi samo u svakom slučaju posebno. Obično će suglasnost utemeljena na informacijama uključivati precizan i vrlo razumljiv opis pitanja za koje se traži suglasnost kao i navođenje posljedica suglasnosti ili nesuglasnosti. Jezik koji se koristi za informiranje treba biti prilagođen predvidivim primateljima informacija.

Informacije također moraju biti lako dostupne osobi čiji se podaci obrađuju. Dostupnost i vidljivost informacija predstavljaju važne elemente. U elektroničkom okruženju dobro rješenje mogu biti slojevite informativne obavijesti jer, osim sažete verzije informacija, osoba čiji se podaci obrađuju može pristupiti i proširenoj verziji.

Posebna suglasnost

Kako bi bila valjana, suglasnost mora također biti posebna, što ide ruku pod ruku s kvalitetom informacija o predmetu suglasnosti. U tom su kontekstu relevantna razumna očekivanja prosječne osobe čiji se podaci obrađuju. Ako treba dodavati ili mijenjati postupke obrade na način koji se nije mogao opravdano predvidjeti u trenutku davanja suglasnosti, od osobe čiji se podaci obrađuju ponovno se mora tražiti suglasnost.

Primjer: U predmetu *Deutsche Telekom AG*,[103] Sud Europske unije bavio se pitanjem je li pružatelj telekomunikacijskih usluga koji je morao proslijediti osobne podatke pretplatnika sukladno članku 12. *Direktive o privatnosti i elektroničkim komunikacijama*[104] trebao zatražiti novu suglasnost osoba čiji se podaci obrađuju jer primatelji u trenutku davanja suglasnosti nisu bili navedeni.

Sud je smatrao da sukladno tom članku nije bila potrebna nova suglasnost za prosljeđivanje podataka jer su osobe čiji se podaci obrađuju, prema toj odredbi, imale mogućnost suglasnosti samo za svrhu obrade, odnosno objavu njihovih podataka, i nisu mogle birati među različitim registrima u kojima su se ti podaci mogli objaviti.

Sud je istaknuo kako „iz kontekstualnog i sustavnog tumačenja članka 12. Direktive o privatnosti i elektroničkim komunikacijama proizlazi da se suglasnost iz članka 12. stavka 2. odnosi na svrhu objave osobnih podataka u javnom registru, a ne na identitet konkretnog pružatelja usluge registra."[105] Nadalje, „sama se objava osobnih podataka u javnom registru posebne svrhe može pokazati štetnom za pretplatnika"[106], a ne konkretan autor takve objave.

103 CJEU, C-543/09, *Deutsche Telekom AG protiv Njemačke*, 5. svibnja 2011.; vidjeti posebno stavke 53. i 54.

104 Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija SL L 2002 L 201 (*Direktiva o privatnosti i elektroničkim komunikacijama*).

105 CJEU, C-543/09, *Deutsche Telekom AG protiv Njemačke*, 5. svibnja 2011.; vidjeti posebno st. 61.

106 *Ibid.*, vidjeti posebno st. 62.

2.4.2. Pravo na povlačenje suglasnosti u svakom trenutku

U Direktivi o zaštiti podataka ne spominje se opće pravo na povlačenje suglasnosti u svakom trenutku. No, općenito se pretpostavlja da takvo pravo postoji i da ga osoba čiji se podaci obrađuju mora biti u mogućnosti koristiti po vlastitom nahođenju. Ne bi se trebali postavljati zahtjevi za obrazloženje povlačenja niti bi smjelo biti rizika ili negativnih posljedica, osim ukidanja svih povlastica koje su proizlazile iz prethodno dogovorene uporabe podataka.

Primjer: Kupac pristane na primanje promidžbenih elektronskih poruka na adresu koju je dostavio nadzorniku. Povuče li kupac suglasnost, nadzornik mora odmah prestati sa slanjem takvih promidžbenih poruka. Ne smiju se nametati bilo kakve kaznene mjere poput plaćanja pristojbi.

Ako je kupac dobivao 5 % popusta na cijenu hotelske sobe kao nagradu što je pristao na korištenje podataka za slanje promidžbenih poruka, naknadno povlačenje suglasnosti za primanje promidžbenih poruka ne bi smjelo imati za posljedicu povrat iznosa popusta.

3

Ključna načela europskog zakonodavstva o zaštiti podataka

EU	Pitanja kojima se bavi	Vijeće Europe
Direktiva o zaštiti podataka, članak 6. stavak 1. točke (a) i (b) CJEU, C-524/06, *Huber protiv Njemačke*, 16. prosinca 2008. CJEU, zajednički slučajevi C-92/09 i C-93/09, *Volker i Markus Schecke GbR (C-92/09) i Hartmut Eifert (C-93/09) protiv Land Hessen*, 9. studenoga 2010.	**Načelo zakonite obrade**	Konvencija br. 108, članak 5. točke (a) i (b) ECtHR, *Rotaru protiv Rumunjske* [GC], br. 28341/95, 4. travnja 2000. ECtHR, *Taylor-Sabori protiv Ujedinjene Kraljevine*, br. 47114/99, 22. listopada 2003. ECtHR, *Peck protiv Ujedinjene Kraljevine*, br. 44647/98, 28. siječnja 2003. ECtHR, *Khelili protiv Švicarske*, br. 16188/07, 18. listopada 2011. ECtHR, *Leander protiv Švedske*, br. 9248/81, 11. srpnja 1985.
Direktiva o zaštiti podataka, članak 6. stavak 1. točka (b)	**Načelo svrhovitosti i ograničenja svrhe**	Konvencija br. 108, članak 5. točka (b)
	Načela kvalitete podataka:	
Direktiva o zaštiti podataka, članak 6. stavak 1. točka (c)	**Relevantnost podataka**	Konvencija br. 108, članak 5. točka (c)

EU	Pitanja kojima se bavi	Vijeće Europe
Direktiva o zaštiti podataka, članak 6. stavak 1. točka (d)	**Točnost podataka**	Konvencija br. 108, članak 5. točka (d)
Direktiva o zaštiti podataka, članak 6. stavak 1. točka (e)	**Ograničeno zadržavanje podataka**	Konvencija br. 108, članak 5. točka (e)
Direktiva o zaštiti podataka, članak 6. stavak 1. točka (e)	**Izuzeće za znanstveno istraživanje i statistiku**	Konvencija br. 108, članak 9. stavak 3.
Direktiva o zaštiti podataka, članak 6. stavak 1. točka (a)	**Načelo poštene obrade**	Konvencija br. 108, članak 5. točka (a) ECtHR, *Haralambie protiv Rumunjske*, br. 21737/03, 27. listopada 2009. ECtHR, *K.H. i drugi protiv Slovačke*, br. 32881/04, 6. studenoga 2009.
Direktiva o zaštiti podataka, članak 6. stavak 2.	**Načelo odgovornosti**	

Načela navedena u članku 5. Konvencije br. 108 sadrže bit europskog zakonodavstva o zaštiti podataka. Pojavljuju se i u članku 6. Direktive o zaštiti podataka kao polazna točka za detaljnije odredbe u sljedećim člancima direktive. Sve kasnije zakonodavstvo o zaštiti podataka na razini Vijeća Europe ili Europske unije mora biti u skladu s tim načelima koja se moraju uzeti u obzir pri tumačenju tog zakonodavstva. Sva izuzeća i ograničenja u pogledu tih ključnih načela moraju biti propisana na nacionalnoj razini;[107] moraju biti zakonom propisana, imati legitimnu svrhu i biti nužna u demokratskom društvu. Sva tri uvjeta moraju biti ispunjena.

3.1. Načelo zakonite obrade

Ključne točke

- Za shvaćanje načela zakonite obrade treba proučiti uvjete za zakonito ograničenje prava na zaštitu podataka u smislu članka 52. stavka 1. Povelje i zahtjeve za opravdano miješanje iz članka 8. stavka 2. Europske konvencije o zaštiti ljudskih prava.

107 Konvencija br. 108, čl. 9. stavak 2.; Direktiva o zaštiti podataka, čl. 13.

- U skladu s tim, obrada je osobnih podataka zakonita samo pod sljedećim uvjetima:
  - u skladu je sa zakonom
  - ima legitimnu svrhu
  - nužna je u demokratskom društvu radi postizanja legitimne svrhe.

Prema zakonodavstvu o zaštiti podataka Europske unije i Vijeća Europe, načelo zakonite obrade prvo je navedeno načelo; na gotovo je jednak način opisano u članku 5. Konvencije br. 108 i u članku 6. Direktive o zaštiti podataka.

Nijedna od tih odredbi ne sadrži definiciju „zakonite obrade". Za shvaćanje tog pravnog pojma treba proučiti pojam opravdanog miješanja iz Europske konvencije o ljudskim pravima kako se tumači u sudskoj praksi Europskog suda za ljudska prava i uvjete za zakonito ograničenje iz članka 52. Povelje.

3.1.1. Zahtjevi za opravdano miješanje iz Europske konvencije o ljudskim pravima

Obrada osobnih podataka može predstavljati miješanje u pravo na poštovanje privatnog života osobe čiji se podaci obrađuju. Međutim, pravo na poštovanje privatnog života nije apsolutno pravo, već se mora uravnotežiti i uskladiti s drugim legitimnim interesima, bilo onima drugih osoba (privatnim interesima) ili onima društva u cjelini (javnim interesima).

Uvjeti u kojima je opravdano miješanje države su sljedeći:

U skladu sa zakonom

Prema sudskoj praksi Europskog suda za ljudska prava, miješanje je u skladu sa zakonom ako se temelji na odredbi nacionalnog zakonodavstva koje ima određene odlike. Zakon mora biti „dostupan dotičnim osobama i njegovi učinci moraju biti predvidivi."[108] Pravilo je predvidivo „ako je formulirano dovoljno precizno da svaki pojedinac – uz, po potrebi, odgovarajuće savjetovanje – može regulirati svoje

108 ECtHR, *Amann protiv Švicarske* [GC], br. 27798/95, 16. veljače 2000., st. 50.; vidjeti također ECtHR, *Kopp protiv Švicarske*, br. 23224/94, 25. ožujka 1998., st. 55. i ECtHR, *Iordachi i drugi protiv Moldavije*, br. 25198/02, 10. veljače 2009., st. 50.

postupanje."[109] „Stupanj preciznosti koji zakon mora imati u tom pogledu ovisi o konkretnom slučaju."[110]

Primjer: U predmetu *Rotaru protiv Rumunjske*,[111] Europski sud za ljudska prava utvrdio je kršenje članka 8. Europske konvencije o ljudskim pravima jer je prema rumunjskom zakonu dopušteno prikupljanje, bilježenje i arhiviranje u tajnim datotekama informacija koje utječu na nacionalnu sigurnost, s time da granice za korištenje tih ovlasti nisu propisane, već ih određuju nadležna tijela. Na primjer, nacionalnim zakonodavstvom nisu definirane vrste informacija koje se smiju obrađivati, kategorije ljudi nad kojima se smiju vršiti mjere nadzora, okolnosti u kojima se takve mjere smiju vršiti niti postupak koji pri tome treba koristiti. Zbog tih je nedostataka Sud zaključio da nacionalno zakonodavstvo nije bilo u skladu sa zahtjevom predvidivosti iz članka 8. Europske konvencije o ljudskim pravima te da je taj članak prekršen.

Primjer: U predmetu *Taylor-Sabori protiv Ujedinjene Kraljevine*,[112] podnositelj je bio podvrgnut nadzoru policije. Koristeći „klon" podnositeljevog dojavljivača policija je presretala poruke koje je primao. Podnositelj je nakon toga uhićen i optužen za zavjeru radi nabave kontrolirane droge. Tužiteljstvo je optužbe protiv podnositelja dijelom temeljilo na zapisima poruka iz dojavljivača koje je transkribirala policija. Međutim, u trenutku kad se podnositelju sudilo, britanskim zakonodavstvom nije bilo regulirano presretanje komunikacije privatnim telekomunikacijskim sustavima. Miješanje u njegova prava dakle nije bilo „u skladu sa zakonom." Europski sud za ljudska prava zaključio je da je prekršen članak 8. Konvencije.

109 ECtHR, *Amann protiv Švicarske* [GC], br. 27798/95, 16. veljače 2000., stavak 56.; vidjeti također ECtHR, *Malone protiv Ujedinjene Kraljevine*, br. 8691/79, 26. travnja 1985., st. 66.; ECtHR, *Silver i drugi protiv Ujedinjene Kraljevine*, brojevi 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. ožujka 1983., st. 88.

110 ECtHR, *The Sunday Times protiv Ujedinjene Kraljevine*, br. 6538/74, 26. travnja 1979., st. 49.; vidjeti također ECtHR, *Silver i drugi protiv Ujedinjene Kraljevine*, brojevi 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. ožujka 1983., st. 88.

111 ECtHR, *Rotaru protiv Rumunjske* [GC], br. 28341/95, 4. travnja 2000., st. 57.; vidjeti također ECtHR, *Udruženje za europske integracije i ljudska prava i Ekimdzhiev protiv Bugarske*, br. 62540/00, 28. lipnja 2007.; ECtHR, *Shimovolos protiv Rusije*, br. 30194/09, 21. lipnja 2011.; i ECtHR, *Vetter protiv Francuske*, br. 59842/00, 31. svibnja 2005.

112 ECtHR, *Taylor-Sabori protiv Ujedinjene Kraljevine*, br. 47114/99, 22. listopada 2002.

Legitimna svrha

Legitimna svrha može se odnositi ili na navedene javne interese ili na prava i slobode drugih.

Primjer: U predmetu *Peck protiv Ujedinjene Kraljevine*,[113] podnositelj je pokušao počiniti samoubojstvo na ulici rezanjem zapešća, pri čemu nije znao da ga snima kamera CCTV-a. Nakon što ga je spasila policija koja je gledala kamere CCTV-a, policijsko je tijelo proslijedilo snimke kamere CCTV-a medijima koji su snimku objavili bez prikrivanja podnositeljeva lica. Europski sud za ljudska prava zaključio je da nadležna tijela nisu imala odgovarajuće ili dovoljne razloge za izravno otkrivanje snimke javnosti bez pristanka podnositelja ili prikrivanja njegova identiteta. Sud je zaključio da je prekršen članak 8. Konvencije.

Nužnost u demokratskom društvu

Eropski sud za ljudska prava istaknuo je da „pojam nužnosti podrazumijeva da je miješanje odgovor na neizbježnu potrebu društva i naročito da je razmjerno legitimnoj svrsi."[114]

Primjer: U predmetu *Khelili protiv Švicarske*,[115] policija je provodeći provjeru utvrdila da podnositeljica posjeduje posjetnice na kojima je pisalo: „Simpatična, zgodna žena u kasnim tridesetima želi upoznati muškarca da se povremeno sastanu uz piće ili zajedno izađu. Broj telefona [...]." Podnositeljica se žalila da ju je policija, nakon pronalaska posjetnice, u svojoj evidenciji zapisala kao prostitutku, iako je ona uporno tvrdila da se time ne bavi. Podnositeljica je zatražila brisanje riječi „prostitutka" iz računalne evidencije policije. Europski sud za ljudska prava potvrdio je da, načelno, zadržavanje osobnih podataka pojedinca zbog mogućnosti da ta osoba počini drugo kazneno djelo u određenim okolnostima može biti razmjerno. Međutim, u podnositeljičinom slučaju, tvrdnja o navodnoj nezakonitoj prostituciji doimala se previše nejasnom i općenitom, nije bila potkrijepljena konkretnim činjenicama jer ona nije nikada bila osuđena za nezakonitu prostituciju pa uvjet „neizbježne društvene potrebe" u smislu članka 8. Konvencije nije bio ispunjen. Smatrajući da su nadležna tijela

113 ECtHR, *Peck protiv Ujedinjene Kraljevine*, br. 44647/98, 28. siječnja 2003., naročito st. 85.

114 ECtHR, *Leander protiv Švedske*, br. 9248/81, 11. srpnja 1985., st. 58.

115 ECtHR, *Khelili protiv Švicarske*, br. 16188/07, 18. listopada 2011.

odgovorna za dokazivanje točnosti pohranjenih podataka o podnositelju i ozbiljnosti narušavanja podnositeljevih prava, Sud je presudio da dugotrajno zadržavanje riječi „prostitutka" u policijskoj evidenciji nije bilo nužno u demokratskom društvu. Sud je zaključio da je prekršen članak 8. Konvencije.

Primjer: U predmetu *Leander protiv Švedske*,[116] Sud je zaključio da tajna provjera osoba koje se prijavljuju za zaposlenje na radnim mjestima važnim za nacionalnu sigurnost nije sama po sebi u suprotnosti sa zahtjevom nužnosti u demokratskom društvu. Posebne zaštitne mjere propisane nacionalnim zakonodavstvom za zaštitu interesa osobe čiji se podaci obrađuju – na primjer, kontrole koje provodi parlament i kancelar za pravosuđe – dovele su do zaključka Suda za ljudska prava da je švedski sustav za kontrolu osoblja ispunio zahtjeve članka 8. stavka 2. Europske konvencije o ljudskim pravima. Imajući na umu da je imala na raspolaganju veliki raspon procjena, tužena država s pravom je smatrala da su u podnositeljevom slučaju interesi nacionalne sigurnosti bili važniji od pojedinačnih. Sud je zaključio da nije prekršen članak 8. Konvencije.

3.1.2. Uvjeti za zakonita ograničenja prema Povelji Europske unije

Struktura i tekst Povelje razlikuju se od strukture i teksta Europske konvencije o ljudskim pravima. U Povelji se ne spominje miješanje u zajamčena prava, no u njoj je sadržana odredba o ograničenju/-ima ostvarivanja prava i sloboda priznatih Poveljom.

Prema članku 52. stavku 1., ograničenja ostvarivanja prava i sloboda priznatih Poveljom i, u skladu s time, ostvarivanja prava na zaštitu osobnih podataka, kao što je obrada osobnih podataka, prihvatljiva su samo pod sljedećim uvjetima:

- propisana su zakonom
- poštuju suštinu prava na zaštitu podataka
- nužna su, podložno načelu razmjernosti
- ispunjavaju ciljeve općeg interesa koje priznaje Unija ili potrebu za zaštitom prava i sloboda drugih.

116 ECtHR, *Leander protiv Švedske*, br. 9248/81, 11. srpnja 1985., st. 59. i 67.

Primjeri: U predmetu *Volker i Markus Schecke*,[117] Sud Europske unije zaključio je da su nametanjem obveze objavljivanja osobnih podataka svih fizičkih osoba koje su bile korisnici potpore iz [određenih poljoprivrednih fondova] bez pravljenja razlike na osnovu bitnih kriterija kao što su razdoblja tijekom kojih su te osobe primale potporu, učestalost ili narav i iznos potpore, Vijeće i Komisija prekoračili ograničenja propisana načelom razmjernosti.

Stoga je Sud Europske unije zaključio da je određene odredbe Uredbe Vijeća (EZ) br. 190/2005 nužno proglasiti nevaljanima, a Uredbu br. 259/2008 proglasiti nevaljanom u cijelosti.[118]

Unatoč drugačijem tekstu, uvjeti za zakonitu obradu iz članka 52. stavka 1. Povelje podsjećaju na članak 8. stavak 2. Konvencije. Štoviše, uvjeti nabrojani u članku 52. stavku 1. Povelje moraju se smatrati sukladnima onima iz članka 8. stavka 2. Konvencije jer se u prvoj rečenici članka 52. stavka 3. navodi da „ako Povelja sadrži prava koja odgovaraju pravima zajamčenima Konvencijom za zaštitu ljudskih prava i temeljnih sloboda, značenje i područje primjene tih prava jednaki su onima iz Konvencije."

Međutim, prema posljednjoj rečenici članka 52. stavka 3, „ta odredba ne sprječava pravo Unije da pruži širu zaštitu." U kontekstu usporedbe članka 8. stavka 2. Konvencije s prvom rečenicom članka 52. stavka 3., to može značiti jedino da su uvjeti za opravdano miješanje u skladu s člankom 8. stavkom 2. Konvencije minimalni zahtjevi za zakonito ograničenje prava na zaštitu podataka u skladu s Poveljom. Stoga je za zakonitu obradu osobnih podataka unutar prava Europske unije potrebno ispuniti najmanje uvjete članka 8. stavka 2. Konvencije; međutim, pravom Europske unije mogli bi se propisati dodatni zahtjevi za posebne slučajeve.

Podudaranje načela zakonite obrade unutar prava Europske unije s odgovarajućim odredbama Konvencije dodatno je učvršćeno člankom 6. stavkom 3. Ugovora o Europskoj uniji kojime se propisuje da „temeljna prava, kako su zajamčena Europskom konvencijom za zaštitu ljudskih prava i temeljnih sloboda [...], čine opća načela prava Unije."

117 CJEU, zajednički slučajevi C-92/09 i C-93/09, *Volker i Markus Schecke GbR (C-92/09) i Hartmut Eifert (C-93/09) protiv Land Hessen*, 9. studenoga 2010., st. 89. i 86.

118 Uredba Vijeća (EZ) br. 1290/2005 od 21. lipnja 2005. o financiranju zajedničke poljoprivredne politike, SL L 2005 L 209; Uredba Komisije (EZ) br. 259/2008 od 18. ožujka 2008. o detaljnim pravilima primjene Uredbe Vijeća (EZ) br. 1290/2005 u pogledu objave informacija o korisnicima sredstava Europskog fonda za jamstva u poljoprivredi (EAGF) i Europskog poljoprivrednog fonda za ruralni razvoj (EAFRD), SL L 2008 L 76.

3.2. Načelo svrhovitosti i ograničenja svrhe

Ključne točke

- Svrha obrade podataka mora se jasno definirati prije početka obrade.
- Unutar prava Europske unije, svrha obrade mora biti izričito utvrđena; unutar prava Vijeća Europe, to je pitanje prepušteno nacionalnom zakonodavstvu.
- Obrada u nedefinirane svrhe nije u skladu sa zakonodavstvom o zaštiti podataka.
- Za daljnju uporabu podataka u druge svrhe potrebna je pravna osnova ako nova svrha obrade nije spojiva s početnom.
- Prijenos podataka na treće stranke je nova svrha za koju je potrebna dodatna pravna osnova.

U suštini, načelo svrhovitosti i ograničenja svrhe znači da legitimnost obrade osobnih podataka ovisi o svrsi obrade.[119] Svrhu mora odrediti i obznaniti nadzornik prije početka obrade podataka.[120] **Unutar prava Europske unije**, to treba učiniti ili putem izjave, odnosno priopćenja, odgovarajućem nadzornom tijelu ili barem putem interne dokumentacije koju nadzornik mora staviti na raspolaganje nadzornim tijelima radi pregleda i osobi čiji se podaci obrađuju radi uvida.

Obrada osobnih podataka za nedefinirane i/ili neograničene svrhe nije zakonita.

Svaka nova svrha obrade podataka mora imati vlastitu zasebnu pravnu osnovu i ne može se oslanjati na činjenicu da su podaci prvotno stečeni ili obrađeni u drugu legitimnu svrhu. Zakonita je obrada pak ograničena na svoju prvotno određenu svrhu pa svaka nova svrha obrade iziskuje novu zasebnu pravnu osnovu. Otkrivanje podataka trećim strankama mora se naročito pažljivo razmotriti jer otkrivanje često predstavlja novu svrhu iziskujući pravnu osnovu različitu od one za prikupljanje podataka.

Primjer: Zračna kompanija prikuplja podatke od svojih putnika radi bilježenja rezervacija i pravilnog upravljanja letom. Zračna kompanija treba podatke o: brojevima sjedala putnika; posebnim tjelesnim ograničenjima, kao što su

119 Konvencija br. 108, čl. 5. točka (b); Direktiva o zaštiti podataka, čl. 6. stavak 1. točka (b).

120 Vidjeti i *Mišljenje 03/2013* Radne skupine iz članka 29. (2013.) *o ograničenju svrhe*, WP 203, Bruxelles, 2. travnja 2013.

potrebe osoba u invalidskim kolicima; i posebnim prehrambenim zahtjevima, kao što su košer ili halal hrana. Ako se od zračne kompanije zatraži prijenos tih podataka, koji se nalaze u evidenciji imena putnika, tijelima nadležnima za imigraciju u odredišnoj zračnoj luci, ti se podaci zatim koriste u svrhu kontrole imigracije koja se razlikuje od početne svrhe prikupljanja podataka. Stoga je za prijenos tih podataka tijelu nadležnom za imigraciju potrebna nova i zasebna pravna osnova.

Pri razmatranju područja primjene i ograničenja određene svrhe, Konvencija br. 108 i Direktiva o zaštiti podataka koriste načelo spojivosti: uporaba podataka u spojive svrhe dopuštena je na temelju početne pravne osnove. Međutim, nije definirano značenje riječi „spojive" u tom kontekstu pa ju je potrebno tumačiti ovisno o slučaju.

Primjer: I Prodaja podataka o kupcima društva Sunshine, koje je društvo steklo tijekom upravljanja odnosima s kupcima (CRM), društvu Moonlight koje se bavi direktnim marketingom, a koje te podatke želi koristiti kao pomoć u marketinškim kampanjama trećih društava, nova je svrha koja nije spojiva s CRM-om, početnom svrhom prikupljanja podataka o kupcima društva Sunshine. Stoga prodaja podataka društvu Moonlight iziskuje vlastitu pravnu osnovu.

Za razliku od toga, uporaba podataka iz CRM-a od strane društva Sunshine u svrhe vlastitog marketinga, odnosno slanje marketinških poruka vlastitim kupcima za vlastite proizvode, općenito je prihvaćena kao spojiva svrha.

U Direktivi o zaštiti podataka izričito je navedeno da se „daljnja obrada osobnih podataka u povijesne, statističke ili znanstvene svrhe ne smatra nespojivom pod uvjetom da države članice osiguraju odgovarajuću zaštitu."[121]

Primjeri: Društvo Sunshine prikupilo je i pohranilo podatke iz CRM-a o svojim kupcima. Društvo Sunshine smije dalje koristiti te podatke radi statističke analize ponašanja svojih kupaca prilikom kupovine jer je statistika spojiva svrha. Nije potrebna daljnja pravna osnova, kao što je suglasnost osobe čiji se podaci obrađuju.

121 Primjer takvih nacionalnih odredbi je austrijski Zakon o zaštiti podataka (*Datenschutzgesetz*), Savezni službeni list I br. 165/1999, st. 46., dostupan na engleskom jeziku na adresi: www.dsk.gv.at/DocView.axd?CobId=41936.

Ako se isti podaci prosljeđuju trećoj stranki, društvu Starlight, u isključivo statističke svrhe, prenošenje bi bilo dopušteno bez dodatne pravne osnove, no samo pod uvjetom da se koriste odgovarajuće zaštitne mjere, kao što je prikrivanje identiteta osoba čiji se podaci obrađuju jer identiteti najčešće nisu nužni za statističke svrhe.

3.3. Načela kvalitete podataka

Ključne točke

- Nadzornik mora primjenjivati načela kvalitete podataka u svim postupcima obrade.
- Na temelju načela ograničenog zadržavanja podataka nužno je podatke izbrisati čim više nisu potrebni u svrhe u koje su prikupljeni.
- Izuzeća od načela ograničenog zadržavanja moraju biti propisana zakonom i iziskuju posebne zaštitne mjere za zaštitu osoba čiji se podaci obrađuju.

3.3.1. Načelo relevantnosti podataka

Obrađuju se samo podaci koji su „primjereni, relevantni i ne prekomjerni u odnosu na svrhu zbog koje se prikupljaju i/ili dalje obrađuju."[122] Kategorije podataka odabranih za obradu moraju biti nužne za postizanje navedenog općeg cilja postupka obrade, a nadzornik treba strogo ograničiti prikupljanje podataka na one informacije koje su izravno relevantne za konkretnu svrhu obrade.

U suvremenom društvu načelo relevantnosti podataka ima dodatni aspekt: korištenjem posebne tehnologije kojom se unapređuje privatnost ponekad je moguće u potpunosti izbjeći uporabu osobnih podataka ili koristiti pseudonimizirane podatke čime se postiže rješenje koje podržava privatnost. To je naročito prikladno u opsežnijim sustavima obrade.

Primjer: Gradsko vijeće redovnim korisnicima sustava gradskog javnog prijevoza nudi čip karticu uz određenu naknadu. Na kartici je navedeno ime korisnika u pisanom obliku, a u čipu u elektroničkom obliku. Pri svakom korištenju autobusa ili tramvaja čip kartica se postavlja ispred ugrađenih uređaja za čitanje, na

122 Konvencija br. 108, čl. 5. točka (c); i Direktiva o zaštiti podataka, čl. 6. stavak 1. točka (c).

primjer, u autobusima i tramvajima. Podaci koje uređaj očita elektronički se provjeravaju u bazi podataka s imenima ljudi koji su kupili putnu kartu.

Ovaj sustav ne poštuje načelo relevantnosti na optimalan način: provjera smije li osoba koristiti sredstva javnog prijevoza mogla bi se izvršiti bez usporedbe osobnih podataka s čip kartice s onima iz baze podataka. Bilo bi dovoljno, na primjer, imati posebnu elektroničku sliku, kao što je bar kod, u čipu kartice kojime bi se, kad se kartica postavi ispred uređaja za čitanje, potvrdila valjanost kartice. Takvim se sustavom ne bi bilježilo tko je i kada koristio prijevozno sredstvo. Ne bi se prikupljali osobni podaci što je optimalno rješenje u smislu načela relevantnosti jer iz tog načela proizlazi obveza smanjenja prikupljanja podataka.

3.3.2. Načelo točnosti podataka

Nadzornik koji raspolaže osobnim podacima ne smije te podatke koristiti bez poduzimanja mjera kojima se može relativno jasno osigurati da su podaci točni i ažurni.

Obvezu osiguravanja točnosti podataka treba promatrati u kontekstu svrhe obrade podataka.

Primjer: Poduzeće koje se bavi prodajom namještaja uzelo je kupčeve podatke o identitetu i adresi radi izdavanja računa. Šest mjeseci kasnije isto je poduzeće htjelo započeti marketinšku kampanju i obratiti se bivšim kupcima. U tom je cilju poduzeće htjelo pristupiti državnom registru stanovnika koji vjerojatno sadrži ažurirane adrese jer su stanovnici zakonom obvezani registru priopćiti svoju trenutačnu adresu. Pristup podacima iz ovog registra ograničen je na osobe i tijela koji za to imaju opravdani razlog.

U ovoj situaciji poduzeće nije moglo iskoristiti argument da mora čuvati točne i ažurirane podatke kako bi dokazalo da ima pravo prikupiti nove podatke o adresama svih svojih bivših kupaca iz registra stanovnika. Podaci su prikupljeni tijekom izdavanja računa; dakle, relevantna je adresa u trenutku prodaje. Nema pravne osnove za prikupljanje novih podataka o adresi jer marketing nije interes koji nadilazi pravo na zaštitu podataka pa se njime ne može opravdati pristup podacima iz registra.

Također mogu postojati slučajevi u kojima je ažuriranje pohranjenih podataka zakonom zabranjeno jer je osnovna svrha pohrane podataka dokumentiranje događaja.

Primjer: Protokol medicinske operacije ne smije se izmijeniti, odnosno „ažurirati", čak i ako se nalazi spomenuti u protokolu kasnije pokažu pogrešnima. U tom se slučaju u protokol smiju samo dodati napomene koje moraju biti jasno označene kao naknadno dodani unosi.

S druge strane, postoje situacije u kojima je redovna provjera točnosti podataka, uključujući ažuriranje, apsolutno nužna zbog moguće štete koju može pretrpjeti osoba čiji se podaci obrađuju ako podaci ostanu netočni.

Primjer: Ako osoba želi sklopiti ugovor s bankovnom institucijom, banka obično provjerava kreditnu sposobnost potencijalnog klijenta. Za to postoje posebne baze podataka u kojima su sadržani podaci o kreditnoj povijesti privatnih osoba. Ako su u takvoj bazi podataka navedeni netočni ili zastarjeli podaci o osobi, ona može imati ozbiljne poteškoće. Voditelji takvih baza podataka stoga se moraju posebno potruditi poštivati načelo točnosti.

Osim toga, podaci koji se ne odnose na činjenice već na sumnje, što je slučaj u kaznenim istragama, mogu se prikupiti i čuvati sve dok nadzornik ima pravnu osnovu za prikupljanje takvih informacija i sve dok su njegove sumnje opravdane.

3.3.3. Načelo ograničenog zadržavanja podataka

Člankom 6. stavkom 1. točkom (e) Direktive o zaštiti podataka, kao i člankom 5. točkom (e) Konvencije br. 108 propisano je da države članice moraju osigurati da se osobni podaci „čuvaju u obliku koji omogućava identifikaciju osoba čiji se podaci obrađuju samo tijekom razdoblja potrebnog u svrhe zbog kojih se podaci prikupljaju ili zbog kojih se dalje obrađuju." Dakle, podaci se moraju izbrisati nakon ispunjavanja tih svrha.

U predmetu *S. and Marper*, Europski sud za ljudska prava zaključio je da ključna načela odgovarajućih instrumenata Vijeća Europe, kao i pravo i praksa drugih ugovornih stranki nalažu da zadržavanje podataka bude razmjerno u odnosu na svrhu prikupljanja i vremenski ograničeno, naročito u policijskim sektoru.[123]

Međutim, vremensko ograničenje za pohranu osobnih podataka odnosi se samo na podatke koji se čuvaju u obliku koji omogućuje identifikaciju osoba čiji se podaci

123 ECtHR, *S. i Marper protiv Ujedinjene Kraljevine*, br. 30562/04 i 30566/04, 4. prosinca 2008.; vidjeti također, na primjer, ECtHR, *M.M. protiv Ujedinjene Kraljevine*, br. 24029/07, 13. studenoga 2012.

obrađuju. Stoga bi se zakonita pohrana podataka koji više nisu potrebni mogla postići anonimizacijom ili pseudonimizacijom podataka.

Čuvanje podataka radi buduće uporabe u znanstvene, povijesne ili statističke svrhe izričito je izuzeto iz načela ograničenog zadržavanja podataka u Direktivi o zaštiti podataka.[124] No, takva kontinuirana pohrana i uporaba osobnih podataka mora biti popraćena posebnim zaštitnim mjerama nacionalnog zakonodavstva.

3.4. Načelo poštene obrade

Ključne točke

- Poštena obrada znači transparentnu obradu, posebno u pogledu osoba čiji se podaci obrađuju.
- Nadzornici moraju obavijestiti osobe čiji se podaci obrađuju prije obrade njihovih podataka, i to barem o svrsi obrade i identitetu i adresi nadzornika.
- Osim ako je to posebno dopušteno zakonom, osobni se podaci ne smiju obrađivati tajno i skriveno.
- Osobe čiji se podaci obrađuju imaju pravo pristupiti svojim podacima gdje god se obrađuju.

Načelom poštene obrade prvenstveno se regulira odnos nadzornika i osobe čiji se podaci obrađuju.

3.4.1. Transparentnost

Ovim se načelom nadzorniku nameće obveza obavješćivanja osoba čiji se podaci obrađuju o načinu uporabe njihovih podataka.

Primjer: U predmetu *Haralambie protiv Rumunjske*,[125] podnositelj je zatražio pristup dosjeu koju je organizacija tajne službe čuvala u vezi s njime, no njegov je zahtjev odobren tek pet godina kasnije. Europski sud za ljudska prava ponovio je da je od vitalne važnosti da pojedinci o kojima javna tijela čuvaju osobne dosjee mogu pristupiti takvim dosjeima. Tijela su bila dužna osigurati učinkovit

124 Direktiva o zaštiti podataka, čl. 6. st. 1. točka (e).

125 ECtHR, *Haralambie protiv Rumunjske*, br. 21737/03, 27. listopada 2009.

postupak dobivanja pristupa takvim informacijama. Sud za ljudska prava smatrao je da niti količina prenesenih dosjea niti nedostaci sustava arhiviranja nisu opravdavali petogodišnje kašnjenje odobravanja podnositeljeva zahtjeva za pristup dosjeima. Tijela podnositelju nisu osigurala učinkovit i pristupačan postupak kojim bi mu se omogućio pristup osobnim dosjeima u razumnom roku. Sud je zaključio da je prekršen članak 8. Konvencije.

Postupci obrade moraju se objasniti osobama čiji se podaci obrađuju na jednostavan i pristupačan način kako bi im se omogućilo da razumiju što će se dogoditi s njihovim podacima. Osoba čiji se podaci obrađuju ima pravo, na zahtjev, od nadzornika saznati obrađuju li se njegovi ili njezini podaci.

3.4.2. Uspostava povjerenja

Nadzornici bi trebali obavijestiti osobe čiji se podaci obrađuju i javnost o tome da će obraditi podatke na zakonit i transparentan način. Postupci obrade ne smiju se provoditi u tajnosti i ne bi smjeli imati nepredvidive negativne učinke. Nadzornici bi trebali osigurati da su kupci, klijenti ili građani obaviješteni o uporabi njihovih podataka. Osim toga, nadzornici moraju postupati na način koji što više odgovara željama osobe čiji se podaci obrađuju, pogotovo ako njegova ili njezina suglasnost predstavlja pravnu osnovu za obradu podataka.

Primjer: U predmetu *K.H. i drugi protiv Slovačke*[126] predstavku je podnijelo osam žena romskog etničkog podrijetla koje su se tijekom trudnoće i poroda liječile u dvjema bolnicama u istočnoj Slovačkoj. Nakon toga nijedna od njih nije mogla ponovno začeti unatoč uzastopnim pokušajima. Nacionalni su sudovi bolnicama naložili da podnositeljicama i njihovim zastupnicima dopuste uvid u njihove zdravstvene kartone i prepisivanje dijelova iz njih, no odbacili su njihov zahtjev da fotokopiraju dokumente navodno zbog sprečavanja zlouporabe. Iz pozitivnih obveza država iz članka 8. Konvencije proizlazila je dužnost da se osobama čiji se podaci obrađuju stave na raspolaganje kopije dosjea s njihovim podacima. Na državi je bilo da odredi načine kopiranja dosjea s osobnim podacima ili, ako je to prikladno, navede uvjerljive razloge uskrate kopiranja. U slučaju podnositeljica, nacionalni su sudovi zabranu kopiranja zdravstvenih kartona prvenstveno opravdali potrebom da se odgovarajuće informacije zaštite od zlouporabe. Međutim, Europski sud za ljudska prava nije mogao shvatiti kako bi podnositeljice, koje su ionako dobile pristup cjelokupnoj zdravstvenoj dokumentaciji,

126 ECtHR, *K.H. i drugi protiv Slovačke*, br. 32881/04, 6. studenoga 2009.

mogle zloupotrijebiti informacije o sebi. Osim toga, rizik od takve zlouporabe mogao se spriječiti na drugačiji način umjesto zabranom podnositeljicama da kopiraju dosjee, na primjer, ograničenjem opsega osoba koje imaju pravo pristupa dosjeima. Država nije uspjela predočiti dovoljno uvjerljive razloge zbog kojih je podnositeljicama zabranjen učinkovit pristup informacijama o njihovom zdravlju. Sud je zaključio da je prekršen članak 8.

Što se tiče internetskih usluga, svojstva sustava za obradu podataka moraju omogućiti osobama čiji se podaci obrađuju da uistinu razumiju što se događa s njihovim podacima.

Poštena obrada također znači da su nadzornici spremni prijeći zakonom propisane minimalne zahtjeve za usluge pružene osobi čiji se podaci obrađuju ako to nalažu legitimni interesi osobe čiji se podaci obrađuju.

3.5. Načelo odgovornosti

Ključne točke

- Odgovornost znači da nadzornici u svojim postupcima obrade podataka moraju aktivno provoditi mjere kojima promiču i štite zaštitu podataka.
- Nadzornici su odgovorni za sukladnost svojih postupaka obrade sa zakonodavstvom o zaštiti podataka.
- Nadzornici bi trebali u svakom trenutku moći dokazati sukladnost s odredbama o zaštiti podataka osobama čiji se podaci obrađuju, javnosti i nadzornim tijelima.

Godine 2013. Organizacija za gospodarsku suradnju i razvoj (OECD) usvojila je smjernice o privatnosti kojima se naglašava da nadzornici imaju važnu ulogu u osiguravanju funkcioniranja zaštite podataka u praksi. Smjernicama se razrađuje načelo odgovornosti na način da „nadzornik treba biti odgovoran za sukladnost s mjerama kojima se provode spomenuta [materijalna] načela."[127]

Dok Konvencija br. 108 ne spominje odgovornost nadzornika, prepuštajući tu temu nacionalnom zakonodavstvu, u članku 6. stavku 2. Direktive o zaštiti podataka

127 OECD (2013), *Smjernice kojima se uređuju zaštita privatnosti i prekogranični prijenosi osobnih podataka*, članak 14.

navedeno je da nadzornik mora osigurati sukladnost s načelima kvalitete podataka iz stavka 1.

Primjer: Primjer iz zakonodavstva kojime se naglašava načelo odgovornosti jest izmjena[128] Direktive o e-privatnosti 2002/58/EZ iz 2009. Prema članku 4. u njegovom izmijenjenom obliku, direktivom se nameće obveza provedbe sigurnosne politike, točnije „osiguravanja provedbe sigurnosne politike u pogledu obrade osobnih podataka." Dakle, u pogledu odredbi o sigurnosti te direktive, zakonodavac je odlučio da je nužno izričito uvjetovati postojanje i provedbu sigurnosne politike.

Prema mišljenju Radne skupine iz članka 29.,[129] suština je odgovornosti obveza nadzornika da:

- uvede mjere kojima bi se – u normalnim okolnostima – jamčilo poštivanje pravila o zaštiti podataka u kontekstu postupaka obrade

- ima spremnu dokumentaciju kojom se osobama čiji se podaci obrađuju i nadzornim tijelima može dokazati koje su mjere poduzete da bi se osigurala sukladnost s pravilima o zaštiti podataka.

Dakle, načelo odgovornosti od nadzornika traži sposobnost aktivnog dokazivanja sukladnosti umjesto čekanja da osobe čiji se podaci obrađuju ili nadzorna tijela ukažu na nedostatke.

128 Direktiva 2009/136/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o izmjeni Direktive 2002/22/EZ o univerzalnoj usluzi i pravima korisnika u vezi s elektroničkim komunikacijskim mrežama i uslugama, Direktiva 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u sektoru elektroničkih komunikacija i Uredba (EZ) br. 2006/2004 o suradnji nacionalnih tijela za provedbu zakona o zaštiti potrošača, SL 337, str. 11.

129 Radna skupina iz članka 29., *Mišljenje 3/2010 o načelu odgovornosti*, WP 173, Bruxelles, 13. srpnja 2010.

4

Pravila europskog zakonoda zaštiti podataka

EU	Pitanja kojima se bavi	Vijeće Europe
Pravila o zakonitoj obradi neosjetljivih podataka		
Direktiva o zaštiti podataka, članak 7. točka (a)	**Suglasnost**	Preporuka o profiliranju, članak 3.4. točka (b) i članak 3.6.
Direktiva o zaštiti podataka, članak 7. točka (b)	**(Pred-)ugovorni odnos**	Preporuka o profiliranju, članak 3.4. točka (b)
Direktiva o zaštiti podataka, članak 7. točka (c)	**Pravne dužnosti nadzornika**	Preporuka o profiliranju, članak 3.4. točka (a)
Direktiva o zaštiti podataka, članak 7. točka (d)	**Vitalni interesi osobe čiji se podaci obrađuju**	Preporuka o profiliranju, članak 3.4. točka (b)
Direktiva o zaštiti podataka, članak 7. točka (e) i članak 8. Stavak 4. CJEU, C-524/06, *Huber protiv Njemačke*, 16. prosinca 2008.	**Javni interes i izvršavanje javne ovlasti**	Preporuka o profiliranju, članak 3.4. točka (b)
Direktiva o zaštiti podataka, članak 7. točka (f) ., članak 8. stavci 2. i 3. CJEU, zajednički slučajevi C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) protiv Administración del Estado*, 24. studenoga 2011.	**Legitimni interesi drugih**	Preporuka o profiliranju, članak 3.4. točka (b)
Pravila o zakonitoj obradi osjetljivih podataka		
Direktiva o zaštiti podataka, članak 8. stavak 1.	**Opća zabrana obrade**	Konvencija br. 108, članak 6.

EU	Pitanja kojima se bavi	Vijeće Europe
Direktiva o zaštiti podataka, članak 8. stavci 2. - 4.	Izuzeća od opće zabrane	Konvencija br. 108, članak 6.
Direktiva o zaštiti podataka, članak 8. stavak 5.	Obrada podataka o (kaznenim) presudama	Konvencija br. 108, članak 6.
Direktiva o zaštiti podataka, članak 8. stavak 7.	Obrada identifikacijskih brojeva	
Pravila sigurne obrade		
Direktiva o zaštiti podataka, članak 17.	Obveza osiguravanja sigurne obrade	Konvencija br. 108, članak 7. ECtHR, *I. protiv Finske*, br. 20511/03, 17. srpnja 2008.
Direktiva o e-privatnosti, članak 4. stavak 2.	Obavješćivanje u slučaju povrede podataka	
Direktiva o zaštiti podataka, članak 16.	Obveza povjerljivosti	
Pravila transparentnosti obrade		
	Transparentnost općenito	Konvencija br. 108, članak 8. točka (a)
Direktiva o zaštiti podataka, članci 10. i 11.	Informacije	Konvencija br. 108, članak 8. točka (a)
Direktiva o zaštiti podataka, članci 10. i 11.	Izuzeća od obveze informiranja	Konvencija br. 108, članak 9.
Direktiva o zaštiti podataka, članci 18. i 19.	Obavješćivanje	Preporuka o profiliranju, članak 9.2. točka (a)
Pravila o promicanju sukladnosti		
Direktiva o zaštiti podataka, članak 20.	Prethodna provjera	
Direktiva o zaštiti podataka, članak 18. stavak 2.	Službenici za zaštitu podataka	Preporuka o profiliranju, članak 8.3.
Direktiva o zaštiti podataka, članak 27.	Pravila ponašanja	

Načela su nužno općenite prirode. Kad se primjenjuju na konkretne situacije, postoje dopuštena tumačenja i izbor sredstava. Unutar **prava Vijeća Europe**, stranke Konvencije br. 108 slobodne su odrediti što je dopušteno tumačenje u svojim nacionalnim zakonodavstvima. U **pravu Europske unije** situacija je drugačija: za uspostavu zaštite podataka na unutarnjem tržištu smatralo se da su, radi usklađivanja razine zaštite podataka nacionalnih zakonodavstava država članica, nužna detaljnija pravila već na razini Europske unije. Direktivom o zaštiti podataka uspostavlja se, prema

načelima navedenima u njezinom članku 6., skup detaljnih pravila koje treba vjerno provesti u nacionalnom zakonodavstvu. Stoga se sljedeće napomene o detaljnim pravilima zaštite podataka na europskoj razini pretežito odnose na pravo Europske unije.

4.1. Pravila zakonite obrade

Ključne točke

- Osobni se podaci mogu zakonito obraditi ako:
  - se obrada temelji na suglasnosti osobe čiji se podaci obrađuju
  - je obrada podataka nužna zbog vitalnih interesa osoba čiji se podaci obrađuju
  - su razlog za obradu legitimni interesi drugih, no samo ako ih ne nadjačavaju interesi zaštite temeljnih prava osoba čiji se podaci obrađuju.
- Zakonita obrada osjetljivih osobnih podataka podliježe posebnom, strožem režimu.

U Direktivi o zaštiti osobnih podataka sadržane su dvije skupine pravila o zakonitoj obradi podataka: jedna za neosjetljive podatke u članku 7. i jedna za osjetljive podatke u članku 8.

4.1.1. Zakonita obrada neosjetljivih podataka

U poglavlju II. Direktive 95/46, naslova „Opća pravila o zakonitosti obrade osobnih podataka", propisano je da, podložno izuzećima iz članka 13., sve obrade osobnih podataka moraju, kao prvo, biti u skladu s načelima u vezi s kvalitetom podataka navedenima u članku 6. Direktive o zaštiti podataka i, kao drugo, s jednim od kriterija za zakonitost obrade podataka navedenim u članku 7.[130] Time se objašnjavaju slučajevi u kojima je zakonito obrađivati neosjetljive osobne podatke.

130 CJEU, zajednički slučajevi C-465/00, C-138/01 i C-139/01 *Österreichischer Rundfunk i drugi*, 20. svibnja 2003., st. 65., CJEU, C-524/06, *Huber protiv Njemačke*, 16. prosinca 2008., st. 48.; CJEU, zajednički slučajevi C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) protiv Administración del Estado*, 24. studenoga 2011., st. 26.

Suglasnost

Unutar prava Vijeća Europe suglasnost se ne spominje ni u članku 8. Europske konvencije o ljudskim pravima ni u Konvenciji br. 108. Spominje se, međutim, u sudskoj praksi Europskog suda za ljudska prava i u nekoliko preporuka Vijeća Europe. **Unutar prava Europske unije**, suglasnost kao osnova za zakonitu obradu podataka jasno je utvrđena člankom 7. točkom (a) Direktive o zaštiti podataka i također se izričito spominje u članku 8. Povelje.

Ugovorni odnos

Druga osnova za zakonitu obradu osobnih podataka **unutar prava Europske unije**, navedena u članku 7. točki (b) Direktive o zaštiti podataka jest da „je obrada potrebna za izvršavanje ugovora kojem je osoba čiji se podaci obrađuju stranka." Ova se odredba odnosi i na predugovorne odnose. Na primjer: stranka namjerava sklopiti ugovor, no to još nije učinila, možda jer je potrebno napraviti još neke provjere. Ako jedna stranka treba obraditi podatke u tu svrhu, takva je obrada zakonita dok god se provodi „kako bi se poduzele mjere na zahtjev osobe čiji se podaci obrađuju prije sklapanja ugovora."

Što se tiče prava Vijeća Europe, „zaštita prava i sloboda drugih" spominje se u članku 8. stavku 2. Europske konvencije o ljudskim pravima kao razlog za zakonito miješanje u pravo na zaštitu podataka.

Pravne dužnosti nadzornika

U **pravu Europske unije** zatim se izričito spominje kriterij zakonitosti obrade podataka, točnije, ako „je obrada potrebna za sukladnost sa zakonskom obvezom kojoj nadzornik podliježe " (članak 7. točka (c) Direktive o zaštiti podataka). Ova se odredba odnosi na nadzornike koji djeluju u privatnom sektoru; pravne obveze nadzornika iz javnog sektora potpadaju pod članak 7. točku (e) Direktive. Mnogo je slučajeva u kojima su nadzornici iz privatnog sektora zakonom dužni obrađivati podatke o drugima; npr. liječnici i bolnice imaju pravnu dužnost pohranjivati podatke o liječenju pacijenata tijekom nekoliko godina, poslodavci moraju obrađivati podatke o svojim zaposlenicima za potrebe socijalnog osiguranja i oporezivanja, a poduzeća moraju obrađivati podatke o svojim klijentima radi oporezivanja.

S obzirom na to da su zračne kompanije dužne prenositi podatke o putnicima stranim tijelima za kontrolu imigracije, postavlja se pitanje mogu li pravne obveze na temelju

stranog zakona predstavljati zakonitu osnovu za obradu podataka unutar prava Europske unije (to je pitanje detaljnije obrađeno u odjeljak 6.2).

Pravne obveze nadzornika predstavljaju osnovu za zakonitu obradu podataka i **unutar prava Vijeća Europe**. Kao što je prethodno navedeno, pravne obveze nadzornika iz privatnog sektora samo su jedan poseban slučaj legitimnih interesa drugih, kao što je navedeno u članku 8. stavku 2. Europske konvencije o ljudskim pravima. Dakle, gornji se primjer odnosi i na pravo Vijeća Europe.

Vitalni interesi osobe čiji se podaci obrađuju

Unutar prava Europske unije, u članku 7. točki (d) **Direktive o zaštiti podataka** propisano je da je obrada osobnih podataka zakonita ako „je potrebna kako bi se zaštitili vitalni interesi osobe čiji se podaci obrađuju." Takvi interesi, koji su usko povezani s preživljavanjem osobe čiji se podaci obrađuju, mogu biti osnova za legitimnu uporabu primjerice zdravstvenih podataka ili podataka o nestalim osobama.

Unutar prava Vijeća Europe, vitalni interesi osoba čiji se podaci obrađuju ne spominju se u članku 8. Europske konvencije o ljudskim pravima kao razlog za zakonito miješanje u pravo na zaštitu podataka. Međutim, u nekim od preporuka Vijeća Europe koje nadopunjuju Konvenciju br. 108 u određenim područjima vitalni interesi osoba čiji se podaci obrađuju izričito su navedeni kao osnova za zakonitu obradu podataka.[131] Čini se da se podrazumijeva da su vitalni interesi osobe čiji se podaci obrađuju jedan od razloga kojima se opravdava obrada podataka: zaštita temeljnih prava ne bi nikad smjela ugroziti vitalne interese štićene osobe.

Javni interes i izvršavanje javne ovlasti

S obzirom na to da se javni poslovi mogu organizirati na mnoge načine, člankom 7. točkom (e) Direktive o zaštiti podataka propisano je da se osobni podaci mogu zakonito obraditi ako „je obrada potrebna za izvršavanje zadatka koji se provodi zbog javnog interesa ili pri izvršavanju javne ovlasti koju ima nadzornik ili treća stranka kojoj se podaci otkrivaju [...]."[132]

131 Preporuka o profiliranju, članak 3. stavak 4. točka (b).

132 Vidjeti također Direktivu o zaštiti podataka, uvodnu izjavu 32.

Primjer: U predmetu *Huber protiv Njemačke*,[133] g. Huber, austrijski državljanin s prebivalištem u Njemačkoj, zatražio je od Saveznog ureda za migracije i izbjeglice da izbriše podatke o njemu u Središnjem registru stranih državljana („AZR"). Taj se registar, u kojemu su sadržani osobni podaci o stanovnicima Europske unije koji nisu njemački državljani, ali borave u Njemačkoj duže od tri mjeseca, koristi u statističke svrhe i od strane policijskih i pravosudnih tijela u istrazi i progonu kriminalnih aktivnosti ili onih koje ugrožavaju javnu sigurnost. Sud koji je proslijedio predmet postavio je pitanje je li obrada osobnih podataka koju obavlja registar poput Središnjeg registra stranih državljana, kojemu mogu pristupiti i druga javna tijela, sukladan s pravom Europske unije s obzirom na to da takav registar ne postoji za njemačke državljane.

Sud Europske unije smatra, kao prvo, da se prema članku 7. točki (e) Direktive osobni podaci mogu zakonito obrađivati samo ako je to potrebno za izvršavanje zadatka koji se provodi zbog javnog interesa ili pri izvršavanju javne ovlasti.

Prema mišljenju Suda, „imajući na umu da je cilj osigurati jednaku razinu zaštite u svim državama članicama, pojam nužnosti iz članka 7. točke (e) Direktive 95/46 [...] ne može imati značenje koje se razlikuje ovisno o državi članici. Iz toga proizlazi da se radi o pojmu koji ima vlastito neovisno značenje u pravu Zajednice i koji treba tumačiti na način kojim se u potpunosti održava cilj te direktive, kako je naveden u njezinom članku 1. stavku [134]

Sud napominje da pravo na slobodu kretanja građana Unije na području države članice čiji nisu državljani nije bezuvjetno, već može podlijegati ograničenjima i uvjetima utvrđenima u Ugovoru i mjerama usvojenima radi njegove provedbe. Dakle, ako je, u načelu, zakonito da država članica koristi registar poput AZR-a radi podrške tijelima odgovornima za primjenu zakonodavstva vezanog uz pravo boravka, takav registar ne smije sadržavati informacije koje nisu potrebne za tu određenu svrhu. Sud je zaključio da je takav sustav obrade osobnih podataka u skladu s pravom Europske unije ako sadrži samo one podatke koji su potrebni za primjenu tog zakonodavstva i ako je zbog njegove centralizirane naravi primjena tog zakonodavstva učinkovitija. Nacionalni sud mora utvrditi jesu li ti uvjeti ispunjeni u ovom konkretnom slučaju. Ako nisu, pohrana i obrada

133 CJEU, C-524/06, *Huber protiv Njemačke*, 16. prosinca 2008.

134 *Ibid.*, st. 52.

osobnih podataka u registru poput AZR-a u statističke svrhe ne mogu se ni po kojoj osnovi smatrati nužnima u smislu članka 7. točke (e) Direktive 95/46/EZ.[135]

Naposljetku, što se tiče pitanja uporabe podataka sadržanih u registru u svrhu suzbijanja kriminala, Sud smatra da taj cilj „nužno uključuje progon počinjenih zločina ili kaznenih djela, neovisno o državljanstvu počinitelja." Predmetni registar ne sadrži osobne podatke vezane uz državljane predmetne države članice i ta razlika u postupanju predstavlja diskriminaciju koja je zabranjena člankom 18. Ugovora o funkcioniranju Europske unije. Stoga se tom odredbom, kako je tumači Sud, „isključuje mogućnost da država članica, u svrhu suzbijanja kriminala, uspostavi sustav za obradu osobnih podataka posebno za stanovnike Unije koji nisu državljani te države članice."[136]

Tijela koja djeluju u javnoj domeni koriste osobne podatke i podložno članku 8. Europske konvencije o ljudskim pravima.

Legitimni interesi nadzornika ili treće stranke

Osoba čiji se podaci obrađuju nije jedina koja ima legitimne interese. Člankom 7. točkom (f) **Direktive o zaštiti podataka** propisano je da se podaci mogu zakonito obraditi ako „je obrada potrebna u svrhe zakonitog interesa kojeg ima nadzornik ili treća stranka ili stranke kojima se podaci otkrivaju, osim kada su ti podaci podređeni interesu za temeljna prava i slobode osobe čiji se podaci obrađuju koja zahtijeva zaštitu [...]."

Sljedeću je sudsku odluku Sud Europske unije donio izričito na temelju članka 7. točke (f) Direktive:

Primjer: U predmetu *ASNEF i FECEMD*,[137] Sud Europske unije pojasnio je da nacionalno zakonodavstvo ne smije dodavati uvjete onima navedenima u članku 7. točki (f) Direktive za zakonitu obradu podataka. To se odnosilo na situaciju u kojoj je španjolski zakon o zaštiti podataka sadržavao odredbu na temelju koje

135 *Ibid.*, st. 54., 58., 59., 66. - 68.

136 *Ibid.*, st. 78. i 81.

137 CJEU, zajednički slučajevi C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) protiv Administración del Estado*, 24. studenoga 2011.

bi druge privatne stranke mogle tvrditi da imaju legitiman interes u obradi osobnih podataka samo ako su se informacije već pojavile u javnim izvorima.

Sud je prvo napomenuo da je cilj Direktive 95/46 osigurati jednaku razinu zaštite prava i sloboda pojedinaca u vezi s obradom osobnih podataka u svim državama članicama. Osim toga, usklađivanjem nacionalnih zakonodavstava u tom području ne smije se osigurati niža razina zaštite. Naprotiv, njima se mora nastojati osigurati visoka razina zaštite u Europskoj uniji.[138] Stoga je Sud Europske unije zaključio da „iz cilja osiguravanja jednake razine zaštite u svim državama članicama proizlazi da se člankom 7. Direktive 95/46 navodi iscrpan i ograničen popis slučajeva u kojima se obrada osobnih podataka može smatrati zakonitom." Osim toga, „države članice ne mogu dodavati nova načela koja se odnose na zakonitost obrade osobnih podataka u članak 7. Direktive 95/46 niti nametati dodatne zahtjeve koji djeluju na način da izmjenjuju opseg primjene jednog od šest načela iz članka 7."[139] Sud je potvrdio da je u pogledu uravnoteženja koje je potrebno prema članku 7. točki (f) Direktive 95/46/EZ, „moguće uzeti u obzir činjenicu da se ozbiljnost povrede temeljnih prava osobe čiji se podaci obrađuju koja proizlaze iz obrade može razlikovati ovisno o tome pojavljuju li se već predmetni podaci u javnim izvorima."

Međutim, „prema članku 7. točki (f) Direktive nije moguće da država članica kategorički i općenito isključi mogućnost obrade određenih vrsta osobnih podataka, a da pri tome ne omogući uzajamno uravnoteženje predmetnih suprotnih prava i interesa u konkretnom slučaju."

S obzirom na navedeno, Sud je zaključio da „članak 7. točku (f) Direktive 95/46 treba tumačiti kao da isključuje nacionalna pravila koja, u slučaju nepostojanja suglasnosti osobe čiji se podaci obrađuju, a radi omogućavanja obrade osobnih podataka osobe čiji se podaci obrađuju koja je nužna da bi se ispunili legitimni interesi nadzornika ili treće stranke ili trećih stranaka kojima se ti podaci otkrivaju, iziskuju ne samo poštovanje temeljnih prava i sloboda osobe čiji se podaci obrađuju, već i pojavljivanje podataka u javnim izvorima. Na taj se način kategorički i općenito isključuje obrada podataka koji se ne pojavljuju u takvim izvorima."[140]

138 *Ibid.*, st. 28. Vidjeti Direktivu o zaštiti podataka, uvodne izjave 8. i 10.

139 CJEU, zajednički slučajevi C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) protiv Administración del Estado*, 24. studenoga 2011., st. 30. i 32.

140 *Ibid.*, st. 40., 44., 48. i 49.

Slične se formulacije nalaze u **preporukama Vijeća Europe.** U Preporuci o profiliranju potvrđuje se da je obrada osobnih podataka u svrhe profiliranja zakonita ako je potrebna radi legitimnih interesa drugih, „osim ako takve interese nadjačavaju temeljna prava i slobode osoba čiji se podaci obrađuju."[141]

4.1.2. Zakonita obrada osjetljivih podataka

Prema **pravu Vijeća Europe** nacionalno zakonodavstvo odgovorno je za utvrđivanje odgovarajuće zaštite za uporabu osjetljivih podataka, dok je u **pravu Europske unije**, u članku 8. Direktive o zaštiti podataka, sadržan detaljan režim obrade vrsta osjetljivih podataka koji otkrivaju: rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja, članstvo u sindikatu ili informacije o zdravlju ili spolnom životu. Obrada osjetljivih podataka u načelu je zabranjena.[142] Međutim, postoji iscrpan popis izuzeća od te zabrane u članku 8. stavcima 2. i 3. Direktive. Ta izuzeća uključuju izričitu suglasnost osobe čiji se podaci obrađuju, vitalne interese osobe čiji se podaci obrađuju, legitimne interese drugih i javni interes.

Za razliku od slučaja obrade neosjetljivih podataka, ugovorni odnos s osobom čiji se podaci obrađuju ne smatra se općom osnovom za zakonitu obradu osjetljivih podataka. Dakle, ako se osjetljivi podaci trebaju obraditi u kontekstu ugovora s osobom čiji se podaci obrađuju, za uporabu tih podataka potrebna je zasebna izričita suglasnost osobe čiji se podaci obrađuju, uz suglasnost za sklapanje ugovora. Izričit zahtjev osobe čiji se podaci obrađuju za robom ili uslugama kojima se nužno otkrivaju osjetljivi podaci ipak se treba smatrati jednako valjanim kao izričita suglasnost.

Primjer: Ako putnik zračne kompanije pri rezervaciji leta od zračne kompanije zatraži invalidska kolica i košer hranu, zračna kompanija smije upotrijebiti te podatke čak i ako putnik nije potpisao posebnu suglasnost u kojoj navodi da dopušta uporabu podataka kojom se otkrivaju informacije o njegovu zdravlju i vjerskim uvjerenjima.

Izričita suglasnost osobe čiji se podaci obrađuju

Prvi uvjet za zakonitu obradu bilo kojih podataka, neosjetljivih ili osjetljivih, jest suglasnost osobe čiji se podaci obrađuju. U slučaju osjetljivih podataka suglasnost mora biti izričita. Međutim, nacionalnim zakonodavstvom može se propisati da

141 Preporuka o profiliranju, članak 3.4. točka (b).

142 Direktiva o zaštiti podataka, čl. 8. st. 1.

davanje suglasnosti za uporabu osjetljivih podataka nije dovoljna pravna osnova za dopuštenje njihove obrade[143] ako, na primjer, u iznimnim slučajevima, obrada uključuje neuobičajene rizike za osobu čiji se podaci obrađuju.

U jednom posebnom slučaju čak se i implicitna suglasnost prihvaća kao pravna osnova za obradu osjetljivih podataka: U članku 8. stavku 2. točki (e) navodi se da obrada nije zabranjena ako se odnosi na podatke koje je osoba čiji se podaci obrađuju jasno obznanila. U toj se odredbi jasno pretpostavlja da se postupanje osobe čiji se podaci obrađuju kojim je objavila svoje podatke mora tumačiti kao da podrazumijeva suglasnost osobe čiji se podaci obrađuju s uporabom tih podataka.

Vitalni interesi osobe čiji se podaci obrađuju

Kao i neosjetljivi podaci, osjetljivi podaci mogu se obraditi zbog vitalnih interesa osobe čiji se podaci obrađuju.[144]

Da bi obrada osjetljivih podataka bila zakonita na toj osnovi, nužno je utvrditi da je bilo nemoguće zatražiti odluku od osobe čiji se podaci obrađuju, jer je osoba čiji se podaci obrađuju, primjerice, bila u nesvijesti ili odsutna i nedostupna.

Legitimni interesi drugih

Kao i u slučaju neosjetljivih podataka, legitimni interesi drugih mogu predstavljati osnovu za obradu osjetljivih podataka. Međutim, u slučaju osjetljivih podataka prema članku 8. stavku 2. Direktive o zaštiti podataka, to se odnosi samo na sljedeće slučajeve:

- ako je obrada potrebna radi vitalnih interesa druge osobe[145] kada osoba čiji se podaci obrađuju nije fizički ili pravno sposobna dati svoju suglasnost

- ako su osjetljivi podaci bitni u području radnog prava, kao što su primjerice zdravstveni podaci bitni u kontekstu posebno opasnog radnog mjesta ili kao što su podaci o vjerskim uvjerenjima bitni primjerice u kontekstu blagdana[146]

143 Ibid., čl. 8. st. 2. točka (a).

144 *Ibid.,* čl. 8. st. 2. točka (c).

145 *Ibid.*

146 *Ibid.,* čl. 8. st. 2. točka (b).

- ako ustanova, udruga ili neko drugo neprofitno tijelo s političkim, filozofskim, vjerskim ili sindikalnim ciljem obrađuju podatke o svojim članovima ili sponzorima ili njihovim interesnim strankama (takvi su podaci osjetljivi jer je velika vjerojatnost da otkrivaju vjerska ili politička uvjerenja dotičnih pojedinaca)[147]

- ako se osjetljivi podaci koriste u kontekstu pravnih postupaka pred sudom ili upravnim tijelom radi podnošenja, provedbe ili obrane pravnog zahtjeva.[148]

- Osim toga, prema članku 8. stavku 3. Direktive o zaštiti podataka, ako zdravstveni radnici koriste zdravstvene podatke za zdravstveni pregled i liječenje, izuzeće se odnosi i na upravljanje tim uslugama. Kao posebna zaštitna mjera, osobe se smatraju „zdravstvenim radnicima" samo ako podliježu posebnim profesionalnim obvezama čuvanja profesionalne tajne.

Javni interes

Osim toga, prema članku 8. stavku 4. Direktive o zaštiti podataka, države članice mogu propisati dodatne svrhe u koje se osjetljivi podaci mogu obrađivati ako:

- se podaci obrađuju zbog značajnog javnog interesa

- je to propisano nacionalnim zakonodavstvom ili odlukom nadzornog tijela

- nacionalno zakonodavstvo ili odluka nadzornog tijela sadrži potrebne zaštitne mjere za učinkovitu zaštitu interesa osoba čiji se podaci obrađuju.[149]

Dobar su primjer elektronički sustavi zdravstvenih kartona koji će se uspostaviti u mnogim državama članicama. Takvi sustavi omogućuju dostupnost zdravstvenih podataka koje prikupljaju zdravstveni radnici tijekom liječenja pacijenta drugim zdravstvenim radnicima tog pacijenta na širokoj osnovi, najčešće nacionalnoj.

Radna skupina iz članka 29. zaključila je da do uspostave takvih sustava ne bi moglo doći prema postojećim zakonskim pravilima za obradu podataka o pacijentima na temelju članka 8. stavka 3. Direktive o zaštiti podataka. Međutim, pod pretpostavkom da postojanje takvih elektroničkih sustava zdravstvenih kartona predstavlja

147 *Ibid.,* čl. 8. st. 2. točka (d).

148 *Ibid.,* čl. 8. st. 2. točka (e).

149 *Ibid.,* čl. 8. st. 4.

značajan javni interes, obrada se može temeljiti na članku 8. stavku 4. Direktive kojim su propisane izričita pravna osnova za njihovu uspostavu i potrebne zaštitne mjere za siguran rad sustava.[150]

4.2. Pravila sigurnosti obrade

Ključne točke

- Pravila sigurnosti obrade podrazumijevaju da su nadzornik i obrađivač obvezni primjenjivati odgovarajuće tehničke i organizacijske mjere radi sprečavanja neovlaštenog ometanja postupaka obrade podataka.
- Nužna razina sigurnosti podataka određuje se prema:
  - sigurnosnim značajkama dostupnima na tržištu za određenu vrstu obrade
  - troškovima
  - osjetljivosti podataka koji se obrađuju.
- Sigurna obrada podataka dodatno je zaštićena time što su sve osobe, nadzornici ili obrađivači, općenito dužni osigurati da podaci ostanu povjerljivi.

Stoga je obveza nadzornika i obrađivača da primjenjuju odgovarajuće mjere sigurnosti podataka navedene u **zakonodavstvu Vijeća Europe o zaštiti podataka** kao i u **zakonodavstvu o zaštiti podataka Europske unije**.

4.2.1. Elementi sigurnosti podataka

Prema odgovarajućim odredbama **prava Europske unije**:

> *„Države članice utvrđuju da nadzornik mora provoditi odgovarajuće tehničke i organizacijske mjere kako bi zaštitio osobne podatke od slučajnog ili nezakonitog uništavanja ili slučajnog gubitka, izmjene, neovlaštenog otkrivanja ili pristupa, posebno kada obrada uključuje prijenos podataka putem mreže, te protiv svih drugih nezakonitih oblika obrade."*[151]

150 Radna skupina iz članka 29. (2007.), *Radni dokument o obradi osobnih podataka vezanih uz zdravlje u elektroničkim zdravstvenim kartonima (EHR)*, WP 131, Bruxelles, 15. veljače 2007.

151 Direktiva o zaštiti podataka, čl. 17. st. 1.

Unutar **prava Vijeća Europe** postoji slična odredba:

> *„Moraju se poduzeti odgovarajuće mjere sigurnosti kako bi se osobni podaci pohranjeni u automatiziranim podatkovnim datotekama zaštitili od slučajnog ili neovlaštenog uništavanja ili slučajnog gubitka kao i od neovlaštenog pristupa, izmjene ili dijeljenja."*[152]

Često su utvrđeni i industrijski, nacionalni i međunarodni standardi sigurne obrade podataka. Na primjer, Europski pečat za zaštitu podataka (EuroPriSe), projekt je transeuropske telekomunikacijske mreže (eTEN) Europske unije kojime su istražene mogućnosti certificiranja proizvoda, naročito softvera, u skladu s europskim zakonodavstvom o zaštiti podataka. Europska agencija za mrežnu i informacijsku sigurnost (ENISA) osnovana je radi unapređivanja sposobnosti Europske unije, država članica Europske unije i poslovne zajednice u pogledu sprečavanja, rješavanja i odgovaranja na poteškoće s mrežnom i informacijskom sigurnošću.[153] ENISA redovno izdaje analize trenutačnih prijetnji u vezi sa sigurnosnom zaštitom i savjete o njihovu rješavanju.

Sigurnost podataka ne postiže se samo primjenom prave opreme – hardvera i softvera. Ona ovisi i o odgovarajućim internim organizacijskim pravilima. Takvim bi internim pravilima idealno bila obuhvaćena sljedeća pitanja:

- redovno pružanje informacija svim zaposlenicima o pravilima sigurnosti podataka i njihovim obvezama prema zakonodavstvu o zaštiti podataka, naročito u pogledu njihovih obveza povjerljivosti
- jasna raspodjela odgovornosti i jasan prikaz stručnih vještina u području obrade podataka, naročito u pogledu odluka o obradi osobnih podataka i prijenosa podataka trećim strankama
- uporaba osobnih podataka samo prema uputama nadležne osobe ili prema općenito utvrđenim pravilima
- zaštita pristupa lokacijama i hardveru i softveru nadzornika ili obrađivača, uključujući provjere ovlaštenja za pristup

152 Konvencija br. 108, čl. 7.

153 Uredba (EZ) br. 460/2004 Europskog parlamenta i Vijeća od 10. ožujka 2004. o osnivanju Europske agencije za mrežnu i informacijsku sigurnost, SL L 2004 L 77.

- osiguravanje da je ovlaštenja za pristup osobnim podacima dodijelila nadležna osoba i zahtijevanje odgovarajuće dokumentacije

- automatizirani protokoli o pristupu osobnim podacima elektroničkim putem i redovne provjere takvih protokola od strane interne nadzorne službe

- pažljivo dokumentiranje drugih oblika otkrivanja osim automatiziranog pristupa podacima kako bi se moglo dokazati da nije došlo ni do kakvih nezakonitih prijenosa podataka.

Ponuda odgovarajuće obuke i obrazovanja o sigurnosti podataka članovima osoblja također je važan element učinkovitih sigurnosnih mjera opreza. Također je potrebno uvesti postupke kojima se provjerava postoje li odgovarajuće mjere samo na papiru ili se one provode i djeluju u praksi (kao što su unutarnje ili vanjske revizije).

Mjere za poboljšanje razine sigurnosti nadzornika ili obrađivača uključuju instrumente kao što su službenici za zaštitu osobnih podataka, obrazovanje zaposlenika o sigurnosti, redovne revizije, ispitivanja probojnosti i pečati kvalitete.

Primjer: U predmetu *I. protiv Finske*,[154] podnositeljica nije uspjela dokazati da su drugi zaposlenici bolnice u kojoj je radila nezakonito pristupili njezinim zdravstvenim kartonima. Stoga su nacionalni sudovi odbacili njezinu tužbu zbog povrede prava na zaštitu podataka. Europski sud za ljudska prava zaključio je da je došlo do kršenja članka 8. Europske konvencije o ljudskim pravima jer bolnički sustav evidencije zdravstvenih kartona „nije omogućio retroaktivno obrazloženje uporabe pacijentovih kartona s obzirom na to da je prikazivao samo pet posljednjih uvida i da su se te informacije brisale nakon vraćanja datoteke u arhivu." Za Sud je od presudne važnosti bilo da bolnički evidencijski sustav očito nije bio u skladu sa zakonskim zahtjevima iz nacionalnog zakonodavstva, čemu nacionalni sudovi nisu pridali dovoljno važnosti.

Obavješćivanje u slučaju povrede podataka

U zakonodavstva o zaštiti podataka nekoliko europskih zemalja uveden je novi instrument za rješavanje povreda zaštite podataka: davatelji elektroničkih komunikacijskih usluga dužni su obavješćivati izgledne žrtve i nadzorna tijela u slučaju

154 ECtHR, *I. protiv Finske*, br. 20511/03, 17. srpnja 2008.

povrede podataka. Davatelje telekomunikacijskih usluga na to obvezuje pravo Europske unije.[155] Osobe čiji se podaci obrađuju obavješćuju se u slučaju povrede podataka radi izbjegavanja štete: obavješćivanja u slučaju povrede podataka i o njihovim mogućim posljedicama smanjuju rizik od negativnih učinaka na osobe čiji se podaci obrađuju. U slučajevima teškog nemara davatelji usluga mogu se i novčano kazniti.

Bit će potrebno unaprijed uspostaviti unutarnje postupke za učinkovito upravljanje i izvješćivanje o kršenju sigurnosti jer je vremenski rok obavješćivanja osoba čiji se podaci obrađuju i/ili nadzornog tijela, prema nacionalnom zakonodavstvu, obično prilično kratak.

4.2.2. Povjerljivost podataka

Unutar prava Europske unije, sigurna obrada podataka dodatno je zaštićena općom dužnošću svih osoba, nadzornika ili obrađivača, u pogledu osiguravanja povjerljivosti podataka.

Primjer: Zaposlenik osiguravajućeg društva na poslu primi poziv od osobe koja tvrdi da je klijent i traži podatke o svojem ugovoru o osiguranju.

S obzirom na to da je dužan podatke klijenata čuvati u tajnosti, zaposlenik mora primijeniti barem minimalne mjere sigurnosti prije otkrivanja osobnih podataka. Način na koji to može učiniti je, na primjer, uzvratnim pozivanjem telefonskog broja zabilježenog u klijentovom dosjeu.

Članak 16. Direktive o zaštiti podataka odnosi se na povjerljivost samo na relaciji nadzornik – obrađivač. Pitanjem dužnosti nadzornika u pogledu povjerljivosti podataka, u smislu da ih ne smiju otkrivati trećim strankama, bave se članci 7. i 8. Direktive.

155 Vidjeti Direktivu 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u sektoru elektroničkih komunikacija, (*Direktiva o privatnosti i elektroničkim komunikacijama*), SL 201, čl. 4. st. 3., kako je izmijenjena Direktivom 2009/136/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o izmjeni Direktive 2002/22/EZ o univerzalnoj usluzi i pravima korisnika u vezi s elektroničkim komunikacijskim mrežama i uslugama; vidjeti također Direktivu 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u sektoru elektroničkih komunikacija i Uredbu (EZ) br. 2006/2004 o suradnji nacionalnih tijela za provedbu zakona o zaštiti potrošača, SL 337.

Obveza povjerljivosti ne odnosi se na situacije u kojima osoba sazna za podatke u svojstvu privatnog pojedinca, a ne zaposlenika nadzornika ili obrađivača. U tom se slučaju ne primjenjuje članak 16. Direktive o zaštiti podataka jer je uporaba osobnih podataka koju provode privatni pojedinci zapravo u potpunosti izuzeta iz područja primjene Direktive s obzirom na to da je unutar granica takozvanog izuzeća za kućanstvo.[156] Izuzeće za kućanstvo je uporaba osobnih podataka „koju provodi fizička osoba tijekom aktivnosti isključivo osobne ili domaće naravi."[157] Nakon odluke Suda Europske unije u predmetu *Bodil Lindqvist*,[158] to se izuzeće, međutim, treba usko tumačiti, naročito u pogledu otkrivanja podataka. Točnije, izuzeće za domaću uporabu ne proširuje se na objavu osobnih podataka neograničenom broju primatelja na internetu (za više pojedinosti o predmetu vidjeti odjeljke 2.1.2, 2.2, 2.3.1 i 6.1).

Unutar prava Vijeća Europe obveza povjerljivosti podrazumijeva se u pojmu sigurnosti podataka iz članka 7. Konvencije br. 108 u kojemu se obrađuje sigurnost podataka.

Za obrađivače povjerljivost znači da osobne podatke koje im je povjerio nadzornik smiju koristiti samo u skladu s uputama koje im je dao nadzornik. Za zaposlenike nadzornika ili obrađivača povjerljivost znači da osobne podatke smiju koristiti samo u skladu s uputama svojih nadležnih nadređenih osoba.

Obveza povjerljivosti mora biti sadržana u svakom ugovoru između nadzornika i njihovih obrađivača. Osim toga, nadzornici i obrađivači moraju poduzeti posebne mjere kako bi za svoje zaposlenike uspostavili pravnu obvezu povjerljivosti. To se obično postiže uključivanjem odredbi o povjerljivosti u ugovor o radu sa zaposlenikom.

Kršenje profesionalnih obveza povjerljivosti kažnjivo je na temelju kaznenog prava u mnogim državama članicama Europske unije i strankama Konvencije br. 108.

156 Direktiva o zaštiti podataka, čl. 3 st. 2. druga alineja.

157 *Ibid.*

158 CJEU, C-101/01, *Bodil Lindqvist*, 6. studenoga 2003.

4.3. Pravila transparentnosti obrade

Ključne točke

- Prije početka obrade osobnih podataka, nadzornik mora barem obavijestiti osobe čiji se podaci obrađuju o identitetu nadzornika i svrsi obrade podataka, osim ako osoba čiji se podaci obrađuju već posjeduje te informacije.
- Ako se podaci prikupljaju od trećih stranaka, obveza davanja informacija ne primjenjuje se ako:
  - je obrada podataka propisana zakonom
  - se davanje informacija pokaže nemogućim ili iziskuje nerazmjeran napor.
- Prije početka obrade osobnih podataka nadzornik mora dodatno:
  - obavijestiti nadzorno tijelo o svojoj namjeri provedbe postupaka obrade
  - imati interno dokumentiranu obradu koju provodi neovisni službenik za zaštitu podataka, ako je nacionalnim zakonodavstvom propisan takav postupak.

Načelo poštene obrade iziskuje transparentnost obrade. U tu svrhu u **pravu Vijeća Europe** propisano je da svaka osoba mora biti u mogućnosti utvrditi postojanje datoteka za obradu podataka, njihovu svrhu i odgovornog nadzornika.[159] Na nacionalnom je zakonodavstvu da utvrdi način na koji bi to trebalo postići. **Pravo Europske unije** je konkretnije pa se osobi čiji se podaci obrađuju transparentnost osigurava obvezom nadzornika da obavijesti osobu čiji se podaci obrađuju, a javnosti se ona osigurava obavješćivanjem.

Unutar obaju pravnih sustava u nacionalnom zakonodavstvu mogu postojati izuzeća i ograničenja od obveze transparentnosti nadzornika ako takvo ograničenje predstavlja mjeru nužnu za zaštitu određenih javnih interesa ili zaštitu osobe čiji se podaci obrađuju ili prava i sloboda drugih ako je to nužno u demokratskom društvu.[160] Takva izuzeća mogu, primjerice, biti potrebna u kontekstu istraživanja zločina, no mogu biti opravdana i u drugim okolnostima.

159 Konvencija br. 108, čl. 8. točka (a).

160 *Ibid*, čl. 9. st. 2.; i Direktiva o zaštiti podataka, čl. 13. st. 1.

4.3.1. Informacije

Prema pravu Vijeća Europe kao i prema pravu Europske unije, nadzornici koji vode postupke obrade obvezni su unaprijed obavijestiti osobu čiji se podaci obrađuju o svojoj namjeri obrade.[161] Ta obveza ne ovisi o zahtjevu osobe čiji se podaci obrađuju, već je nadzornik mora proaktivno poštivati, bez obzira na to pokazuje li osoba čiji se podaci obrađuju zanimanje za informacije.

Sadržaj informacija

Informacije moraju sadržavati svrhu obrade kao i identitet i kontaktne podatke nadzornika.[162] Prema Direktivi o zaštiti podataka potrebno je dati daljnje informacije „ako su takve daljnje informacije potrebne, uzimajući u obzir posebne okolnosti u kojima se informacije prikupljaju, radi osiguravanja poštene obrade u odnosu na osobu čiji se podaci obrađuju." U člancima 10. i 11. Direktive navedene su, među ostalim, vrste podataka koji se obrađuju i primatelji takvih podataka, kao i postojanje prava na pristup i ispravljanje podataka. Ako se podaci prikupljaju od osoba čiji se podaci obrađuju, informacije bi trebale objašnjavati jesu li odgovori na pitanja obvezni ili dobrovoljni, kao i moguće posljedice neodgovaranja.[163]

Sa stajališta **prava Vijeća Europe**, davanje takvih informacija može se smatrati dobrom praksom prema načelu poštene obrade podataka pa je do te mjere također dio prava Vijeća Europe.

Prema načelu poštene obrade informacije moraju biti lako razumljive osobama čiji se podaci obrađuju. Mora se koristiti jezik koji odgovara primateljima. Razina i vrsta korištenog jezika mora se razlikovati ovisno o tome jesu li informacije namijenjene, na primjer, odraslima ili djeci, javnosti ili stručnom akademskog osoblju.

Neke osobe čiji se podaci obrađuju htjet će samo jezgrovite informacije o načinu i razlogu za obradu njihovih podataka, dok će druge htjeti detaljno objašnjenje. Način na koji se taj aspekt poštenog informiranja može uravnotežiti razmatra se u mišljenju Radne skupine iz članka 29. kojim se zagovara ideja takozvanih slojevitih

161 Konvencija br. 108, čl. 8. točka (a); i Direktiva o zaštiti podataka, čl. 10. i 11.

162 Konvencija br. 108, čl. 8. točka (a); i Direktiva o zaštiti podataka, čl. 10. točke (a) i (b).

163 Direktiva o zaštiti podataka, čl. 10. točka (c).

obavijesti.[164] Onim osobama čiji se podaci obrađuju omogućuju da same odluče o iscrpnosti informacija.

Vrijeme pružanja informacija

U Direktivi o zaštiti podataka sadržane su ponešto drugačije odredbe o vremenu pružanja informacija, ovisno o tome prikupljaju li se podaci od osobe čiji se podaci obrađuju (članak 10.) ili od treće stranke (članak 11.). Ako se podaci prikupljaju od osobe čiji se podaci obrađuju, informacije treba pružiti najkasnije u trenutku prikupljanja. Ako se podaci prikupljaju od trećih stranaka, informacije treba pružiti najkasnije ili u trenutku kad nadzornik zabilježi podatke ili prije prvog otkrivanja podataka trećoj stranki.

Izuzeća od obveze informiranja

Unutar prava Europske unije opće izuzeće od obveze informiranja osobe čiji se podaci obrađuju vrijedi u slučaju kad osoba čiji se podaci obrađuju već posjeduje informacije.[165] To se odnosi na situacije u kojima je osoba čiji se podaci obrađuju, ovisno o okolnostima slučaja, već svjesna toga da njezine podatke nadzornik već obrađuje u određenu svrhu.

U članku 11. Direktive, koji se odnosi na obvezu informiranja osobe čiji se podaci obrađuju ako podaci nisu dobiveni od nje, također se navodi da takva obveza ne vrijedi, naročito u slučajevima obrade u statističke svrhe ili u svrhe povijesnog ili znanstvenog istraživanja, kada:

- je davanje takvih informacija nemoguće
- ili ako bi uključivalo nerazmjerni napor
- ili ako je bilježenje ili otkrivanje izričito propisano zakonom.[166]

Samo je u članku 11. stavku 2. Direktive o zaštiti podataka navedeno da osobe čiji se podaci obrađuju ne treba informirati o postupcima obrade ako su propisani

164 Radna skupina iz članka 29. (2004.), *Mišljenje 10/2004 o usklađenijem pružanju informacija*, WP 100, Bruxelles, 25. studenoga 2004.

165 Direktiva o zaštiti podataka, čl. 10. i čl. 11. st. 1.

166 *Ibid*, uvodna izjava 40. i članak 11. st. 2.

zakonom. S obzirom na opću pravnu pretpostavku da osobe na koje se zakon odnosi poznaju zakon, može se smatrati da je, ako su podaci prikupljeni od osobe čiji se podaci obrađuju prema članku 10. Direktive, osoba čiji se podaci obrađuju informirana. No, s obzirom na to da se poznavanje zakona samo pretpostavlja, člankom 10. propisano je da se na temelju načela poštene obrade osoba čiji se podaci obrađuju treba informirati čak i ako je obrada propisana zakonom, pogotovo jer informiranje osobe čiji se podaci obrađuju nije naročito zahtjevno ako se podaci prikupljaju izravno od osobe čiji se podaci obrađuju.

Što se tiče **prava Vijeća Europe**, Konvencijom br. 108 izričito su propisana izuzeća iz njezina članka 8. Izuzeća navedena u člancima 10. i 11. Direktive o zaštiti podataka mogu se smatrati primjerima dobre prakse za izuzeća iz članka 9. Konvencije br. 108.

Različiti načini pružanja informacija

Idealan način pružanja informacija bio bi obraćanje svakoj pojedinoj osobi čiji se podaci obrađuju, usmenim ili pisanim putem. Ako se podaci prikupljaju od osobe čiji se podaci obrađuju, davanje informacija treba ići ruku pod ruku s prikupljanjem. Međutim, informacije se mogu pružati i odgovarajućim objavljivanjem, naročito ako se podaci prikupljaju od trećih stranaka, s obzirom na očite praktične poteškoće osobnog kontaktiranja s osobama čiji se podaci obrađuju.

Jedan od najučinkovitijih načina pružanja informacija jest putem odgovarajućih informacijskih klauzula na naslovnici internetske stranice nadzornika, kao što je politika zaštite privatnosti internetske stranice. Međutim, znatan dio stanovništva ne koristi internet što bi društvo ili javno tijelo trebalo uzeti u obzir u svojoj politici informiranja.

4.3.2. Obavješćivanje

Nacionalnim zakonodavstvom može se nadzornike obvezati na obavješćivanje nadležnog nadzornog tijela o njihovim postupcima obrade kako bi se mogli objaviti. Isto tako, nacionalnim se zakonodavstvom može propisati da nadzornici mogu zaposliti službenika za zaštitu podataka koji je naročito odgovoran za vođenje registra o postupcima obrade koje provodi nadzornik.[167] Taj se interni registar treba staviti na raspolaganje javnosti na zahtjev bilo koje osobe.

167 *Ibid.,* čl. 18. st. 2. druga alineja.

Primjer: U obavijesti i u dokumentaciji internog službenika za zaštitu podataka trebaju biti opisana glavna svojstva predmetnog postupka obrade. To uključuje informacije o nadzorniku, svrsi obrade, pravnoj osnovi obrade, vrsti podataka koji se obrađuju, vjerojatnim primateljima trećim strankama i o tome postoji li namjera prekograničnih prijenosa podataka i, ako postoji, kojih.

Nadzorno tijelo mora obavijesti objavljivati u obliku posebnog registra. Kako bi se ispunila njegova svrha, pristup tom registru treba biti jednostavan i besplatan. Isto vrijedi za dokumentaciju za koju je zadužen službenik za zaštitu podataka nadzornika.

Izuzeća od obveze obavješćivanja nadležnog nadzornog tijela ili angažiranja internog službenika za zaštitu podataka mogu se propisati nacionalnim zakonodavstvom za postupke obrade za koje je izgledno da neće predstavljati poseban rizik za osobe čiji se podaci obrađuju. Ta su izuzeća navedena u članku 18. stavku 2. Direktive o zaštiti podataka.[168]

4.4. Pravila o promicanju sukladnosti

Ključne točke

- U razradi načela odgovornosti, u Direktivi o zaštiti podataka spominje se nekoliko instrumenata za promicanje sukladnosti:
  - prethodna provjera planiranih postupaka obrade od strane nacionalnog nadzornog tijela
  - službenici za zaštitu podataka koji nadzorniku pružaju posebno znanje u području zaštite podataka
  - pravila ponašanja u kojima se navode postojeća pravila za zaštitu podataka za primjenu u grani društva, naročito poslovanja.
- U pravu Vijeća Europe, u Preporuci o profiliranju, predloženi su slični instrumenti za promicanje sukladnosti.

168 *Ibid.,* čl. 18. st. 2. prva alineja.

4.4.1. Prethodna provjera

Prema članku 20. Direktive o zaštiti podataka, nadzorno tijelo mora provjeriti postupke obrade koji bi mogli predstavljati poseban rizik za prava i slobode osoba čiji se podaci obrađuju – bilo zbog svrhe ili zbog okolnosti obrade – prije početka obrade. Nacionalnim se zakonodavstvom mora odrediti koje se postupke obrade može prethodno provjeriti. Posljedica takve provjere može biti zabrana postupaka obrade ili nalog da se promjene značajke predloženog plana postupaka obrade. Cilj članka 20. Direktive jest osigurati da do nepotrebno rizične obrade niti ne dođe jer je nadzorno tijelo ovlašteno zabraniti takve postupke. Da bi taj mehanizam bio učinkovit, nadzorno tijelo mora doista biti obaviješteno. Kako bi osigurala da nadzornici ispunjavaju svoju obvezu obavješćivanja, nadzorna tijela moraju imati ovlasti prisile. Jedna je od njih izricanje novčanih kazni nadzornicima.

Primjer: Ako društvo obavlja postupke obrade koji prema nacionalnom zakonodavstvu podliježu prethodnoj provjeri, to društvo nadzornom tijelu mora podnijeti dokumentaciju o planiranim postupcima obrade. Društvo ne smije započeti postupke obrade prije pozitivnog odgovora nadzornog tijela.

U nekim državama članicama nacionalnim je zakonodavstvom alternativno propisano da postupci obrade mogu započeti ako nadzorno tijelo ne reagira u određenom roku, na primjer, tromjesečnom.

4.4.2. Službenici za zaštitu podataka

Direktiva o zaštiti podataka također ostavlja mogućnost da se nacionalnim zakonodavstvom propiše da nadzornici mogu imenovati službenika koji će djelovati kao službenik za zaštitu podataka.[169] Cilj je tog službenika osigurati da postupci obrade ne ugrožavaju prava i slobode osoba čiji se podaci obrađuju.[170]

Primjer: U Njemačkoj, prema odjeljku 4f, pododjeljku 1. njemačkog Saveznog zakona o zaštiti podataka (*Bundesdatenschutzgesetz*) društva u privatnom vlasništvu moraju imenovati internog službenika za zaštitu podataka ako trajno zapošljavaju 10 ili više osoba u automatiziranoj obradi osobnih podataka.

169 *Ibid.,* čl. 18. st. 2. druga alineja.

170 *Ibid.*

Za postizanje tog cilja službenik mora imati određenu razinu neovisnosti unutar organizacije nadzornika, kako je izričito istaknuto u Direktivi. Kako bi se podržala učinkovitost njegove službe, potrebna su i čvrsta radna prava kojima se zaposlenici štite od primjerice neopravdanog otkaza.

Radi promicanja sukladnosti s nacionalnim zakonodavstvom o zaštiti podataka, pojam internih službenika za zaštitu podataka usvojen je i u nekim od preporuka Vijeća Europe.[171]

4.4.3. Pravila ponašanja

Radi promicanja sukladnosti, poslovni i drugi sektori mogu sastaviti detaljna pravila kojima reguliraju svoje uobičajene postupke obrade i na taj način kodificirati najbolje prakse. Stručno znanje članova sektora pomoći će u pronalasku praktičnih rješenja za koje je izgledno da će biti prihvaćena. Sukladno tome, države članice i Komisija potiču se na promicanje izrade pravila ponašanja s ciljem doprinošenja pravilnoj provedbi nacionalnih odredbi koje države članice usvoje u skladu s direktivom, uzimajući u obzir posebne značajke različitih sektora.[172]

Kako bi osigurale sukladnost tih pravila ponašanja s nacionalnim odredbama usvojenima u skladu s Direktivom o zaštiti podataka, države članice moraju uspostaviti postupak evaluacije pravila. U taj je postupak obično potrebno uključiti nacionalno tijelo, trgovinske udruge i druga tijela koja predstavljaju druge kategorije nadzornika.[173]

Prijedlozi pravila Zajednice i izmjene ili proširenja postojećih pravila Zajednice mogu se dostaviti radi evaluacije Radnoj skupini iz članka 29. Nakon što ih Radna skupina odobri, Europska komisija može osigurati odgovarajuću promidžbu tih pravila.[174]

Primjer: Europska federacija direktnog i interaktivnog marketinga (FEDMA) razvila je Europski kodeks prakse za uporabu osobnih podataka u direktnom marketingu. Kodeks je uspješno dostavljen Radnoj skupini iz članka 29.

171 Vidjeti primjerice Preporuku o profiliranju, čl. 8. st. 3.

172 Vidjeti Direktivu o zaštiti podataka, čl. 27. st. 1.

173 *Ibid.,* čl. 27. st. 2.

174 *Ibid.,* čl. 27. st. 3.

Kodeksu je 2010. dodan prilog koji se odnosi na elektroničke marketinške komunikacije.[175]

175 Radna skupina iz članka 29. (2010.), *Mišljenje 4/2010 o Europskom kodeksu ponašanja FEDMA-e za uporabu osobnih podataka u direktnom marketingu*, WP 174, Bruxelles, 13. srpnja 2010.

5

Prava osobe čiji se podaci obrađuju i njihova provedba

EU	Pitanja kojima se bavi	Vijeće Europe
Pravo na pristup		
Direktiva o zaštiti podataka, članak 12. CJEU, C-553/07, *College van burgemeester en wethouders van Rotterdam protiv M.E.E. Rijkeboer*, 7. svibnja 2009.	**Pravo na pristup vlastitim podacima**	Konvencija br. 108, članak 8. točka (b)
	Pravo na ispravljanje, brisanje ili blokiranje	Konvencija br. 108, članak 8. točka (c) ECtHR, *Cemalettin Canli protiv Turske*, br. 22427/04, 18. studenoga 2008. ECtHR, *Segerstedt-Wiberg i drugi protiv Švedske*, br. 62332/00, 6. lipnja 2006. ECtHR, *Ciubotaru protiv Moldavije*, br. 27138/04, 27. travnja 2010.
Pravo na prigovor		
Direktiva o zaštiti podataka, članak 14. stavak 1. točka (a)	**Pravo na prigovor zbog posebne situacije osobe čiji se podaci obrađuju**	Preporuka o profiliranju, članak 5.3.
Direktiva o zaštiti podataka, članak 14. stavak 1. točka (b)	**Pravo na prigovor na daljnju uporabu podataka u marketinške svrhe**	Preporuka o direktnom marketingu, članak 4.1.
Direktiva o zaštiti podataka, članak 15.	**Pravo na prigovor na automatizirane odluke**	Preporuka o profiliranju, članak 5.5.

EU	Pitanja kojima se bavi	Vijeće Europe
Neovisni nadzor		
Povelja, članak 8. stavak 3. Direktiva o zaštiti podataka, članak 28. Institucije Europske unije, poglavlje V. Uredba o zaštiti podataka CJEU, C-518/07, *Europska komisija protiv Savezne Republike Njemačke*, 9. ožujka 2010. CJEU, C-518/10, *Europska komisija protiv Republike Austrije*, 16. listopada 2012. CJEU, C-288/12, *Tužba podnesena 8. travnja 2012. – Europska komisija protiv Mađarske*, 8. lipnja 2012.	**Nacionalna nadzorna tijela**	Konvencija br. 108, Dodatni protokol, članak 1.
Pravni lijekovi i sankcije		
Direktiva o zaštiti podataka, članak 12.	**Zahtjev nadzorniku**	Konvencija br. 108, članak 8. točka (b)
Direktiva o zaštiti podataka, članak 28. stavak 4. Uredba o zaštiti podataka u institucijama Europske unije, članak 32. stavak 2.	**Zahtjevi podneseni nadzornom tijelu**	Konvencija br. 108, Dodatni protokol, članak 1. stavak 2. točka (b)
Povelja, članak 47.	**Sudovi (općenito)**	Europska konvencija o ljudskim pravima, članak 13.
Direktiva o zaštiti podataka, članak 28. stavak 3.	**Nacionalni sudovi**	Konvencija br. 108, Dodatni protokol, članak 1. stavak 4.
Ugovor o funkcioniranju Europske unije, članak 263. stavak 4. Uredba o zaštiti podataka u institucijama Europske unije, članak 32. stavak 1. Ugovor o funkcioniranju Europske unije, članak 267.	**Sud Europske unije**	
	Europski sud za ljudska prava	Europska konvencija o ljudskim pravima, članak 34.
Pravni lijekovi i sankcije		
Povelja, članak 47. Direktiva o zaštiti podataka, članci 22. i 23. CJEU, C-14/83, *Sabine von Colson i Elisabeth Kamann protiv Land Nordrhein-Westfalen*, 10. travnja 1984. CJEU, C-152/84, *M.H. Marshall protiv Southamptona i Zdravstvene ustanove za područje jugozapadnog Hampshirea*, 26. veljače 1986.	**Za kršenja nacionalnog zakonodavstva o zaštiti podataka**	Europska konvencija o ljudskim pravima, članak 13. (samo za države članice Vijeća Europe) Konvencija br. 108, članak 10. *ECtHR, K.U. protiv Finske*, br. 2872/02, 2. ožujka 2008. ECtHR, *Biriuk protiv Litve*, br. 23373/03, 25. studenog 2008.

EU	Pitanja kojima se bavi	Vijeće Europe
Uredba o zaštiti podataka u institucijama Europske unije, članci 34. i 49. CJEU, C-28/08 P, *Europska komisija protiv The Bavarian Lager Co. Ltd*, 29. lipnja 2010.	Za kršenja prava Europske unije od strane institucija i tijela Europske unije	

Učinkovitost pravnih propisa općenito, a posebno prava osoba čiji se podaci obrađuju, u velikoj mjeri ovisi o postojanju odgovarajućih mehanizama za njihovu provedbu. U europskom zakonodavstvu o zaštiti podataka, osoba čiji se podaci obrađuju mora imati pravo zaštititi svoje podatke na temelju nacionalnog zakonodavstva. Nacionalnim zakonodavstvom treba uspostaviti i neovisna nadzorna tijela koja će osobama čiji se podaci obrađuju pomoći u ostvarivanju prava i nadzirati obradu osobnih podataka. Osim toga, pravo na učinkoviti pravni lijek, zajamčeno Europskom konvencijom o ljudskim pravima i Poveljom, znači da pravni lijekovi moraju biti dostupni svakoj osobi.

5.1. Prava osoba čiji se podaci obrađuju

Ključne točke

- Prema nacionalnom zakonodavstvu svaka osoba mora imati pravo zatražiti informacije od nadzornika o tome obrađuje li nadzornik njezine podatke.
- Na temelju nacionalnog zakonodavstva osobe čiji se podaci obrađuju imaju pravo na:
  - pristup vlastitim podacima od nadzornika koji takve podatke obrađuje
  - ispravak (ili blokiranje, ovisno o slučaju) svojih podataka, ako su netočni, koji provodi nadzornik koji obrađuje njihove podatke
  - brisanje ili blokiranje, ovisno o slučaju, svojih podataka koje provodi nadzornik ako nadzornik podatke obrađuje nezakonito.
- Osim toga, osobe čiji se podaci obrađuju imaju pravo na prigovor nadzornicima u vezi s:
  - automatiziranim odlukama (koje se donose na temelju osobnih podataka koji su obrađeni samo automatski)
  - obradom svojih podataka ako to dovodi do nerazmjernih rezultata
  - uporabom svojih podataka u svrhu direktnog marketinga.

5.1.1. Pravo na pristup

Unutar prava Europske unije, u članku 12. Direktive o zaštiti podataka, sadržani su elementi prava osobe čiji se podaci obrađuju na pristup, uključujući pravo da od nadzornika dobije „potvrdu obrađuju li se ili ne podaci koji se na nju odnose, te podatak barem u vezi svrhe obrade, vrste podataka, te primatelje ili vrste primatelja kojima se podaci otkrivaju," kao i „ispravak, brisanje ili blokiranje podataka čija obrada nije u skladu s ovom Direktivom, posebno zbog nepotpunih ili netočnih podataka."

Unutar prava Vijeća Europe postoje ista ta prava koja se moraju propisati nacionalnim zakonodavstvom (članak 8. Konvencije br. 108). U nekoliko se preporuka Vijeća Europe koristi pojam „pristup" uz opis različitih vidova prava na pristup i prijedlog za provedbu u nacionalnom zakonodavstvu i to na isti način naveden u prethodnom stavku.

Prema članku 9. Konvencije br. 108 i članku 13. Direktive o zaštiti podataka, obveza nadzornika da odgovore na zahtjev za pristupom osobe čiji se podaci obrađuju može se ograničiti zbog prevladavajućih pravnih interesa drugih. Prevladavajući pravni interesi mogu uključivati javne interese kao što su nacionalna sigurnost, javna sigurnost i progon kaznenih djela, kao i privatne interese koji su snažniji od interesa zaštite podataka. Sva izuzeća ili ograničenja moraju biti nužna u demokratskom društvu i razmjerna cilju. U vrlo iznimnim slučajevima, na primjer zbog medicinskih indikacija, zaštita osobe čiji se podaci obrađuju može sama po sebi iziskivati ograničenje transparentnosti; to se naročito odnosi na ograničenje prava na pristup svake osobe čiji se podaci obrađuju.

Kad god se podaci obrađuju isključivo u svrhu znanstvenog istraživanja ili u statističke svrhe, Direktivom o zaštiti podataka omogućeno je ograničenje prava pristupa nacionalnim zakonodavstvom. U tom slučaju, međutim, valja uspostaviti odgovarajuće zaštitne mjere. Naročito treba osigurati da se ne donose ikakve mjere ili odluke vezano uz bilo kojeg pojedinca u kontekstu takve obrade podataka i da „nema rizika od kršenja privatnosti osobe čiji se podaci obrađuju."[176] Slične su odredbe sadržane u članku 9. stavku 3. Konvencije br. 108.

Pravo na pristup vlastitim podacima

Unutar prava Vijeća Europe, pravo na pristup vlastitim podacima izričito je potvrđeno člankom 8. Konvencije br. 108. Europski sud za ljudska prava opetovano je

176 Direktiva o zaštiti podataka, čl. 13. st. 2.

tvrdio da postoji pravo na pristup informacijama o vlastitim podacima koje drugi čuvaju ili koriste, i da to pravo proizlazi iz potrebe za poštovanjem privatnog života.[177] U predmetu *Leander*,[178] Europski sud za ljudska prava zaključio je da pravo na pristup osobnim podacima koje čuvaju javna tijela ipak može biti ograničeno u određenim okolnostima.

Unutar prava Vijeća Europe, pravo na pristup vlastitim podacima izričito je potvrđeno člankom 12. Direktive o zaštiti podataka, a kao temeljno pravo člankom 8. stavkom 2. Povelje.

U članku 12. točki (a) propisano je da države članice moraju jamčiti pravo na pristup osobnim podacima i informacijama svakoj osobi čiji se podaci obrađuju. Točnije, svaka osoba čiji se podaci obrađuju ima pravo od nadzornika dobiti potvrdu obrađuju li se podaci koji se na nju odnose i informacije koje pokrivaju barem sljedeće:

- svrhu obrade
- vrstu predmetnih podataka
- podatke koji se obrađuju
- primatelje ili vrste primatelja kojima se podaci otkrivaju
- sve dostupne informacije o izvoru podataka koji se obrađuju
- u slučaju automatiziranih odluka, logiku automatske obrade podataka.

Nacionalnim zakonodavstvom mogu se dodati informacije koje treba pružiti nadzornik. Tu spada primjerice navođenje pravne osnove za obradu podataka.

Primjer: Pristupom vlastitim osobnim podacima osoba može utvrditi jesu li podaci točni pa osobu čiji se podaci obrađuju obavezno treba informirati o vrstama podataka koji se obrađuju te o sadržaju podataka. Nije dakle dovoljno da nadzornik naprosto kaže osobi čiji se podaci obrađuju da obrađuje njezino

177 ECtHR, *Gaskin protiv Ujedinjene Kraljevine*, Nbr. 10454/83, 7. srpnja 1989.; *Odièvre protiv Francuske* [GC], br. 42326/98, 13. veljače 2003.; ECtHR, *K.H. i drugi protiv Slovačke*, br. 32881/04, 28. travnja 2009.; ECtHR, *Godelli protiv Italije*, br. 33783/09, 25. rujna 2012.

178 ECtHR, *Leander protiv Švedske*, br. 9248/81, 11. srpnja 1985.

ime, adresu, datum rođenja i područje interesa. Nadzornik mora osobi čiji se podaci obrađuju otkriti i da obrađuje „ime: N.N.; adresu: 1040 Beč, Schwarzenbergplatz 11, Austrija; datum rođenja: 10.10.1974.; i područje interesa (prema izjavi osobe čiji se podaci obrađuju): klasična glazba." Posljednja stavka dodatno sadrži informacije o izvoru podataka.

Obavješćivanje osobe čiji se podaci obrađuju o podacima koji se obrađuju i o svim dostupnim informacijama o izvoru podataka koji se obrađuju mora biti provedeno u razumljivom obliku, što znači da će nadzornik možda morati osobi čiji se podaci obrađuju detaljnije objasniti predmet obrade. Na primjer, nije dovoljno samo navesti tehničke kratice ili medicinske pojmove u odgovoru na zahtjev za pristupom, čak i ako su pohranjene samo takve kratice ili pojmovi.

Ako su dostupne, informacije o izvoru podataka koje obrađuje nadzornik treba navesti u odgovoru na zahtjev za pristupom. Ovu odredbu treba promatrati u svjetlu načela poštene obrade i odgovornosti. Nadzornik ne smije uništiti informacije o izvoru podataka kako ih ne bi morao otkrivati niti zanemariti standardne i priznate potrebe za dokumentacijom u području svojih aktivnosti. Ako nadzornik ne čuva nikakvu dokumentaciju o izvoru podataka koji se obrađuju, to najčešće neće značiti da je ispunio svoje obveze u vezi s pravom na pristup.

Ako se provode automatizirane evaluacije, treba objasniti opću logiku evaluacije, uključujući kriterije koji su razmatrani u evaluaciji osobe čiji se podaci obrađuju.

U Direktivi nije jasno opisano odnosi li se pristup informacijama na prošlost i, ako je tako, na koje razdoblje u prošlosti. U tom pogledu, kako je utvrđeno sudskom praksom Suda Europske unije, pravo na pristup vlastitim podacima ne smije se nepotrebno vremenski ograničiti. Osobama čiji se podaci obrađuju također treba dati razumnu mogućnost dobivanja informacija o prošlim postupcima obrade podataka.

Primjer: U predmetu *Rijkeboer*,[179] od Suda Europske unije zatraženo je da utvrdi može li se, prema članku 12. točki (a) Direktive, pravo pojedinca na pristup informacijama o primateljima ili vrstama primatelja osobnih podataka i o sadržaju priopćenih podataka ograničiti na godinu dana prije njegova zahtjeva za pristupom.

179 CJEU, C-553/07, *College van burgemeester en wethouders van Rotterdam protiv M.E.E. Rijkeboer*, 7. svibnja 2009.

Kako bi utvrdio je li na temelju članka 12. točke (a) Direktive dopušteno takvo vremensko ograničenje, Sud je odlučio tumačiti taj članak u svjetlu svrha Direktive. Sud je prvo istaknuo da je pravo na pristup nužno kako bi osoba čiji se podaci obrađuju mogla ostvariti svoje pravo da nadzornik ispravi, izbriše ili blokira njezine podatke (članak 12. točka (b)), ili obavijesti treće stranke kojima su podaci otkriveni o toj ispravci, brisanju ili blokiranju (članak 12. točka (c)). Pravo na pristup nužno je i kako bi se osobi čiji se podaci obrađuju dala mogućnost da ostvari svoje pravo na prigovor na obradu osobnih podataka (članak 14.) ili pravo na tužbu ako pretrpi štetu (članci 22. i 23.).

Radi osiguravanja praktičnog učinka gore spomenutih odredbi, Sud je smatrao da se „to pravo mora obavezno odnositi na prošlost. U suprotnom osoba čiji se podaci obrađuju ne bi mogla učinkovito ostvariti svoje pravo na ispravak, brisanje ili blokiranje podataka koji se smatraju nezakonitima ili netočnima, odnosno na pokretanje sudskog postupka i naknadu za pretrpljenu štetu."

Pravo na ispravak, brisanje i blokiranje podataka

„Svaka osoba mora biti u mogućnosti ostvariti pravo na pristup podacima koji se na nju odnose i u postupku su obrade, naročito kako bi provjerila točnost podataka i zakonitost obrade."[180] U skladu s tim načelima, osobe čiji se podaci obrađuju prema nacionalnom zakonodavstvu moraju imati pravo na ispravak, brisanje ili blokiranje svojih podataka, koje treba provesti nadzornik, ako smatraju da obrada nije u skladu s odredbama direktive, naročito zbog netočnosti ili nepotpunosti podataka.[181]

Primjer: U predmetu *Cemalettin Canli protiv Turske*,[182] Europski sud za ljudska prava utvrdio je kršenje članka 8. Europske konvencije o ljudskim pravima u netočnom policijskom izvješću u kaznenom postupku.

Podnositelj je dvaput bio podvrgnut kaznenom postupku zbog navodnog članstva u nezakonitim organizacijama, no nikad nije bio osuđen. Kad je podnositelj ponovno uhićen i optužen za još jedno kazneno djelo, policija je kaznenom sudu predala izvješće pod naslovom *„obrazac s informacijama o dodatnim kaznenim djelima"*, u kojemu se podnositelj pojavljivao kao član dviju nezakonitih

180 Direktiva o zaštiti podataka, uvodna izjava 41.

181 *Ibid.*, čl. 12. točka (b).

182 ECtHR, *Cemalettin Canli protiv Turske*, br. 22427/04, 18. studenoga 2008., stavci 33. , 42. i 43.; ECtHR, *Dalea protiv Francuske*, br. 964/07, 2. veljače 2010.

organizacija. Zahtjev podnositelja za izmjenom izvješća i policijske evidencije bio je neuspješan. Europski sud za ljudska prava smatrao je da su informacije u policijskom izvješću bile u okviru članka 8. Europske konvencije o ljudskim pravima jer bi javne informacije također mogle spadati u kategoriju „privatnog života" ako se sustavno prikupljaju i pohranjuju u datotekama koje čuvaju nadležna tijela. Osim toga, policijsko izvješće bilo je netočno, a njegovo sastavljanje i podnošenje kaznenom sudu nije bilo u skladu sa zakonom. Sud je zaključio da je prekršen članak 8.

Primjer: U predmetu *Segerstedt-Wiberg i drugi protiv Švedske*,[183] podnositelji su bili povezani s određenim liberalnim i komunističkim političkim strankama. Sumnjali su na to da su informacije o njima unesene u sigurnosnu policijsku evidenciju. Europski sud za ljudska prava zadovoljio se činjenicom da je pohrana predmetnih podataka imala pravnu osnovu i legitimnu svrhu. U pogledu nekih podnositelja Europski sud za ljudska prava utvrdio je da je kontinuirano zadržavanje podataka predstavljalo nerazmjerno miješanje u njihove privatne živote. Na primjer, u slučaju g. Schmida, nadležna su tijela zadržala informaciju da je 1969. navodno zagovarao nasilan otpor policijskoj kontroli tijekom demonstracija. Europski sud za ljudska prava utvrdio je da te informacije nisu mogle biti ni u kakvom interesu nacionalne sigurnosti, naročito s obzirom na to da se odnose na prošlost. Europski sud za ljudska prava zaključio je da je prekršen članak 8. Konvencije u pogledu četvorice od petorice podnositelja.

U nekim je slučajevima dovoljno da osoba čiji se podaci obrađuju jednostavno zatraži ispravak, na primjer, pravopisne greške u imenu, promjenu adrese ili broja telefona. Međutim, ako su takvi zahtjevi povezani s pravnim pitanjima, kao što je pravni identitet osobe čiji se podaci obrađuju ili točno mjesto stanovanja radi dostave pravnih dokumenata, zahtjevi za ispravcima možda neće biti dovoljni i nadzornik će moći zatražiti dokaz navodne netočnosti. Takvim se zahtjevima osobi čiji se podaci obrađuju ne smije nametnuti nerazuman teret dokaza, onemogućujući osobama čiji se podaci obrađuju ispravak njihovih podataka. Europski sud za ljudska prava utvrdio je kršenja članka 8. Europske konvencije o ljudskim pravima u nekoliko slučajeva u kojima podnositelj nije mogao opovrgnuti točnost informacija iz tajnih registara.[184]

183 ECtHR, *Segerstedt-Wiberg i drugi protiv Švedske*, br. 62332/00, 6. lipnja 2006., stavci 89. i 90.; vidjeti također, na primjer, ECtHR, *M.K. protiv Francuske*, br. 19522/09, 18. travnja 2013.

184 ECtHR, *Rotaru protiv Rumunjske*, br. 28341/95, 4. svibnja 2000.

Primjer: U predmetu *Ciubotaru protiv Moldavije*,[185] podnositelj nije mogao promijeniti upis svojeg etničkog podrijetla u službenoj evidenciji s moldavskog na rumunjsko navodno zbog toga što je propustio potkrijepiti svoj zahtjev. Europski sud za ljudska prava smatrao je da je prihvatljivo da države zatraže objektivan dokaz pri upisu etničkog podrijetla pojedinca. Ako se takav zahtjev temelji isključivo na subjektivnim i nepotkrijepljenim temeljima, nadležna tijela mogu ga odbiti. Međutim, podnositeljev zahtjev nije bio utemeljen samo na subjektivnom poimanju vlastitog etničkog podrijetla. On je iznio svoje veze s rumunjskom etničkom skupinom koje su se mogle objektivno provjeriti, na primjer jezik, ime, empatija i drugo. Međutim, prema nacionalnom zakonodavstvu, podnositelj je morao osigurati dokaze da su njegovi roditelji pripadali rumunjskoj etničkoj skupini. S obzirom na povijesnu situaciju u Moldaviji, takav je zahtjev stvorio nepremostivu prepreku upisu etničkog identiteta koji bi se razlikovao od onog upisanog za njegove roditelje koji je zabilježila sovjetska vlast. Budući da je podnositelju onemogućila pregled njegovog zahtjeva u svjetlu dokaza koji se mogu objektivno provjeriti, država je propustila ispuniti svoju pozitivnu dužnost osiguravanja učinkovitog poštovanja privatnog života podnositelja. Sud je zaključio da je prekršen članak 8. Konvencije.

Tijekom građanskog postupka ili postupka pred javnim tijelom u kojem se odlučuje o točnosti podataka, osoba čiji se podaci obrađuju može zatražiti bilježenje naznake ili napomene o osporavanju točnosti i čekanju službene odluke u svojoj podatkovnoj datoteci. U tom razdoblju nadzornik ne smije podatke predstavljati kao sigurne ili konačne, naročito trećim strankama.

Zahtjev osobe čiji se podaci obrađuju za brisanjem ili blokiranjem podataka često se temelji na tvrdnji da obrada podataka nema zakonitu osnovu. Takve se tvrdnje obično pojavljuju kad se suglasnost povuče ili kad određeni podaci više nisu potrebni za ispunjavanje svrhe prikupljanja podataka. Teret dokaza da je obrada podataka zakonita snosi nadzornik jer je on odgovoran za zakonitost obrade. Prema načelu odgovornosti, nadzornik mora u svakom trenutku moći dokazati da postoji čvrsta pravna osnova za obradu podataka. U suprotnom se obrada mora prekinuti.

Ako se obrada podataka osporava zbog navodne netočnosti podataka ili nezakonitosti obrade, osoba čiji se podaci obrađuju, u skladu s načelom poštene obrade, može zatražiti blokiranje spornih podataka. To znači da se podaci ne brišu, već da se nadzornik mora suzdržati od uporabe podataka tijekom razdoblja blokade. To je naročito

185 ECtHR, *Ciubotaru protiv Moldavije*, br. 27138/04, 27. travnja 2010., st. 51. i 59.

potrebno kad kontinuirana uporaba netočnih ili nezakonito čuvanih podataka može naštetiti osobi čiji se podaci obrađuju. Nacionalnim se zakonodavstvom treba osigurati više pojedinosti o tome kad može nastati obveza blokiranja uporabe podataka i način na koji se provodi.

Osobe čiji se podaci obrađuju imaju dodatno pravo od nadzornika dobiti obavijest trećim strankama o svakom blokiranju, ispravcima ili brisanju, ako su podatke primili prije tih postupaka obrade. Budući da je nadzornik trebao dokumentirati otkrivanje podataka trećim strankama, treba postojati mogućnost identificiranja primatelja podataka i zahtijevanja brisanja. Međutim, ako su podaci u međuvremenu objavljeni, na primjer, na internetu, može ih biti nemoguće izbrisati u svim slučajevima jer primatelje podataka nije moguće naći. Prema Direktivi o zaštiti podataka, obavezno je kontaktirati s primateljima podataka radi ispravka, brisanja ili blokiranja podataka, „osim ako se to pokaže nemogućim ili uključuje nerazmjeran napor."[186]

5.1.2. Pravo na prigovor

Pravo na prigovor uključuje pravo na prigovor na automatizirane pojedinačne odluke, pravo na prigovor zbog posebne situacije osobe čiji se podaci obrađuju i pravo na prigovor na daljnju obradu podataka u svrhu direktnog marketinga.

Pravo na prigovor na automatizirane pojedinačne odluke

Automatizirane su odluke one donesene na temelju osobnih podataka koji su obrađeni isključivo automatskim sredstvima. Ako je za takve odluke vjerojatno da će znatno utjecati na živote pojedinaca jer se odnose, na primjer, na kreditnu sposobnost, poslovnu učinkovitost, ponašanje ili pouzdanost, nužna je posebna zaštita radi izbjegavanja neprimjerenih posljedica. U Direktivi o zaštiti podataka propisano je da se automatiziranim odlukama ne trebaju određivati pitanja koja su važna za pojedince i da pojedinac treba imati pravo na pregled automatizirane odluke.[187]

Primjer: Važan praktičan primjer automatiziranog donošenja odluka je ocjenjivanje kreditne sposobnosti. Radi brzog odlučivanja o kreditnoj sposobnosti budućeg klijenta, određeni podaci, kao što su zanimanje i obiteljska situacija, prikupljaju se od klijenta i kombiniraju s podacima o osobi čiji se podaci obrađuju dostupnima iz drugih izvora, kao što su sustavi kreditnih informacija. Ti se

186 Direktiva o zaštiti podataka, čl. 12. točka (c), druga polovica rečenice.

187 *Ibid.,* čl. 15. st. 1.

podaci automatski učitavaju u algoritam za ocjenjivanje koji izračunava ukupnu vrijednost koja predstavlja kreditnu sposobnost potencijalnog klijenta. Na taj način zaposlenik društva može u nekoliko sekundi odlučiti je li osoba čiji se podaci obrađuju prihvatljiva kao klijent.

Unatoč tome, prema Direktivi države članice moraju osigurati da se osoba može podvrgnuti automatiziranoj pojedinačnoj odluci ako interesi osobe čiji se podaci obrađuju nisu ugroženi jer je odluka u korist osobe čiji se podaci obrađuju, ili su zaštićeni drugim odgovarajućim sredstvima.[188] Pravo na prigovor na automatizirane odluke također je sadržano u **pravu Vijeća Europe** što je vidljivo iz Preporuke o profiliranju.[189]

Pravo na prigovor zbog posebne situacije osobe čiji se podaci obrađuju

Ne postoji opće pravo osoba čiji se podaci obrađuju na prigovor na obradu njihovih podataka.[190] Međutim, prema članku 14. točki (a) Direktive o zaštiti podataka, osoba čiji se podaci obrađuju ima pravo podnijeti prigovor temeljeći ga na uvjerljivoj pravnoj osnovi koja se tiče posebne situacije osobe čiji se podaci obrađuju. Slično se pravo priznaje u Preporuci o profiliranju Vijeća Europe.[191] Cilj je takvih odredbi pronaći najbolju ravnotežu između prava osobe čiji se podaci obrađuju na zaštitu svojih podataka i legitimnih prava drugih u postupku obrade podataka osobe čiji se podaci obrađuju.

Primjer: Banka podatke o svojim klijentima koji ne izvršavaju kreditnu obvezu pohranjuje sedam godina. Klijent čiji su podaci pohranjeni u toj bazi podataka traži novi kredit. Provjerava se baza podataka, ocjenjuje se financijska situacija i klijentu se odbija kredit. Međutim, klijent može uložiti prigovor na evidentiranje njegovih osobnih podataka u bazi podataka i zatražiti brisanje podataka ako može dokazati da je neizvršavanje kreditne obveze bio samo rezultat pogreške koja je ispravljena odmah nakon što je klijent za nju saznao.

188 *Ibid.,* čl. 15. st. 2.

189 Preporuka o profiliranju, čl. 5. st. 5.

190 Vidjeti također ECtHR, *M.S. protiv Švedske*, br. 20837/92, 27. kolovoza 1997., u kojemu su medicinski podaci priopćeni bez suglasnosti ili mogućnosti prigovora; ili ECtHR, *Leander protiv Švedske*, br. 9248/81, 26. ožujka 1987.; ili ECtHR, *Mosley protiv Ujedinjene Kraljevine*, br. 48009/08, 10. svibnja 2011.

191 Preporuka o profiliranju, čl. 5. st. 3.

Učinak uspješnog prigovora jest da nadzornik više ne smije obrađivati predmetne podatke. Međutim, postupci obrade podataka osobe čiji se podaci obrađuju prije prigovora i dalje su zakoniti.

Pravo na prigovor na daljnju uporabu podataka u svrhu direktnog marketinga

Člankom 14. točkom (b) Direktive o zaštiti podataka propisano je posebno pravo na prigovor na uporabu podataka određene osobe u svrhu direktnog marketinga. Takvo je pravo utvrđeno i u preporuci Vijeća Europe o direktnom marketingu.[192] Takav se prigovor ulaže prije nego što podaci postanu dostupni trećim strankama u svrhu direktnog marketinga. Stoga osoba čiji se podaci obrađuju mora imati mogućnost prigovora prije prijenosa podataka.

5.2. Neovisni nadzor

Ključne točke

- Radi osiguravanja učinkovite zaštite podataka, nacionalnim zakonodavstvom moraju biti uspostavljena neovisna nadzorna tijela.
- Nacionalna nadzorna tijela moraju djelovati potpuno neovisno, a neovisnost im se mora zajamčiti pravom na temelju kojeg su uspostavljena i mora se odražavati u posebnoj organizacijskog strukturi nadzornog tijela.
- Nadzorna tijela imaju, među ostalim, sljedeće posebne zadaće:
  - nadzirati i promicati zaštitu podataka na nacionalnoj razini
  - savjetovati osobe čiji se podaci obrađuju i nadzornike kao i vladu i čitavu javnost
  - saslušati prigovore i pomoći osobi čiji se podaci obrađuju u vezi s navodnim kršenjem prava na zaštitu podataka
  - nadzirati nadzornike i obrađivači
  - intervenirati, po potrebi,
    - upozoravanjem, opominjanjem ili čak novčanim kažnjavanjem nadzornika i obrađivača

192 Vijeće Europe, Odbor ministara (1985), Preporuka Rec(85)20 državama članicama o zaštiti osobnih podataka koji se koriste u svrhu direktnog marketinga, 25. listopada 1985., čl. 4. st. 1.

  - izdavanjem naloga da se podaci isprave, blokiraju ili izbrišu
  - nametanjem zabrane obrade
- uputiti slučajeve sudu.

Prema Direktivi o zaštiti podataka neovisan je nadzor nužan kao važan mehanizam za osiguravanje učinkovite zaštite podataka. Direktivom je uveden instrument za provedbu zaštite podataka koji se prvotno nije pojavio u Konvenciji br. 108 niti u Smjernicama OECD-a o privatnosti.

S obzirom na to da se neovisan nadzor pokazao neizostavnim za razvoj učinkovite zaštite podataka, u novoj se odredbi revidiranih Smjernica OECD-a o privatnosti usvojenih 2013. države članice poziva na „uspostavu i održavanje tijela za provedbu privatnosti koja bi imala upravu, izvore i tehničko znanje nužne za učinkovito ostvarivanje svojih ovlasti i objektivno, nepristrano i dosljedno odlučivanje."[193]

Unutar **prava Vijeća Europe**, prema Dodatnom protokolu o Konvenciji br. 108 uspostava nadzornih tijela postala je obvezna. U tom je instrumentu, u članku 1., sadržan pravni okvir za neovisna nadzorna tijela koji ugovorne stranke moraju provesti u svojem nacionalnom zakonodavstvu. U njemu se koriste formulacije za opis zadaća i ovlasti tih tijela slične onima iz Direktive o zaštiti podataka. Stoga bi nadzorna tijela u načelu trebala funkcionirati na jednak način unutar prava Europske unije i onog Vijeća Europe.

Unutar **prava Europske unije**, nadležnost i organizacijska struktura nadzornih tijela najprije su navedene u članku 28. stavku 1. Direktive o zaštiti podataka. Uredbom o zaštiti podataka u institucijama Europske unije[194] uspostavlja se Europski nadzornik za zaštitu podataka i nadzorno tijelo za obradu podataka koju provode tijela i institucije Europske unije. Navodeći uloge i odgovornosti nadzornog tijela Uredba se oslanja na iskustvo prikupljeno od objave Direktive o zaštiti podataka.

Neovisnost tijela za zaštitu podataka zajamčena je člankom 16. stavkom 2. Ugovora o funkcioniranju Europske unije i člankom 8. stavkom 3. Povelje. U toj se posljednjoj

193 OECD (2013), Smjernice kojima se uređuju zaštita privatnosti i prekogranični prijenosi osobnih podataka, st. 19. točka (c).

194 Uredba (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka SL L 2001 L 8, čl. 41. - 48.

odredbi kontrola neovisnog tijela smatra ključnim elementom temeljnog prava na zaštitu podataka. Osim toga, prema Direktivi o zaštiti podataka, države članice moraju uspostaviti nadzorna tijela radi nadzora primjene Direktive pri čemu moraju djelovati potpuno neovisno.[195] Zakonodavstvo na kojem se temelji osnivanje nadzornog tijela mora sadržavati odredbe koje ponajprije jamče neovisnost, a konkretna organizacijska struktura tijela mora biti dokaz njegove neovisnosti.

Godine 2010. Sud Europske unije prvi se put bavio pitanjem opsega primjene zahtjeva za neovisnošću nadzornih tijela za zaštitu podataka.[196] Sljedeći primjeri ilustriraju način njegova razmišljanja.

Primjer: U predmetu *Komisija protiv Njemačke*,[197] Europska komisija zatražila je od Suda Europske unije izjavu da je Njemačka netočno prenijela zahtjev „potpune neovisnosti" nadzornih tijela odgovornih za osiguravanje zaštite podataka ne ispunivši na taj način svoje obveze iz članka 28. stavka 1. Direktive o zaštiti podataka. Sa stajališta Komisije, problem je bio u tome što je Njemačka stavila pod nadzor države tijela odgovorna za nadzor obrade osobnih podataka izvan javnog sektora u različitim saveznim državama (*Länder*).

Procjena suštine toga postupka ovisila je, prema mišljenju Suda, o opsegu primjene zahtjeva za neovisnošću iz te odredbe, a time i njezinom tumačenju.

Sud je istaknuo da se riječi „potpuno neovisno" iz članka 28. stavka 1. Direktive moraju tumačiti na temelju stvarnog teksta te odredbe i na temelju ciljeva i sheme Direktive o zaštiti podataka.[198] Sud je naglasio da su nadzorna tijela „čuvari" prava vezanih uz obradu osobnih podataka koja se jamče Direktivom te da je stoga njihova uspostava u državama članicama „ključni element zaštite pojedinaca u pogledu obrade osobnih podataka."[199] Sud je zaključio da „u izvršavanju svojih obveza nadzorna tijela moraju postupati objektivno i nepristrano. Zbog toga, osim utjecaja nadziranih tijela, nadzorna tijela moraju biti lišena i

195 Direktiva o zaštiti podataka, posljednja rečenica članka 28. stavka 1.; Konvencija br. 108, Dodatni protokol, čl. 1. st. 3.

196 Vidjeti FRA (2010); *Temeljna prava: izazovi i postignuća u 2010.*, Godišnje izvješće za 2010., st. 59. Agencija Europske unije za temeljna prava to je pitanje detaljnije obradila u svojem izvješću o *Zaštiti podataka u Europskoj uniji: uloga nacionalnih tijela nadležnih za zaštitu podataka*, koje je objavljeno u svibnju 2010.

197 CJEU, C-518/07, *Europska komisija protiv Savezne Republike Njemačke*, 9. ožujka 2010., st. 27.

198 *Ibid.*, st. 17. i 29.

199 *Ibid.*, st. 23.

svih ostalih vanjskih utjecaja, uključujući izravan ili neizravan utjecaj države ili *Länder*."[200]

Sud Europske unije također je utvrdio da značenje „potpune neovisnosti" treba tumačiti u svjetlu neovisnosti Europskog nadzornika za zaštitu podataka kako je definirana u Uredbi o zaštiti podataka u institucijama Europske unije. Kako je istaknuo Sud, u njezinom članku 44. stavku 2. objašnjen je pojam neovisnosti dodavanjem dijela o tome da Europski nadzornik za zaštitu podataka provodeći svoje dužnosti ne smije tražiti ili primati upute ni od koga." Time je isključena mogućnost da država nadzire neovisno nadzorno tijelo za zaštitu podataka.[201]

Zbog toga je Sud Europske unije smatrao da njemačke institucije za zaštitu podataka na razini savezne države nadležne za nadzor obrade osobnih podataka koju provode nejavna tijela nisu bile dovoljno neovisne jer ih je nadzirala država.

Primjer: U predmetu *Komisija protiv Austrije*,[202] Sud Europske unije naglasio je slične probleme u vezi s položajem određenih članova i osoblja austrijskog tijela za zaštitu podataka (Komisija za zaštitu podataka, DSK). Sud je u ovom slučaju zaključio da je na temelju austrijskog zakonodavstva isključena mogućnost da austrijsko tijelo za zaštitu podataka izvršava svoje dužnosti potpuno neovisno u smislu Direktive o zaštiti podataka. Neovisnost austrijskog tijela za zaštitu podataka nije bila osigurana u dostatnoj mjeri jer Savezni kancelar DSK-u osigurava radnu snagu, nadzire DSK i ima se pravo u svakom trenutku informirati o njegovu radu.

Primjer: U predmetu *Komisija protiv Mađarske*,[203] Sud Europske unije je istaknuo da „zahtjev [...] za jamčenje da svako nadzorno tijelo bude imalo mogućnost provođenja povjerenih zadaća potpuno nezavisno, uključuje obvezu konkretne države članice da osigura potpuno trajanje mandata". Sud je također naveo da „prijevremenim okončanjem mandata čelnika nadzornog tijela za zaštitu osobnih podataka, Mađarska je propustila izvršiti svoje obveze iz Direktive 95/46/EZ [...]."

200 *Ibid.*, st. 25.

201 *Ibid.*, st. 27.

202 CJEU, C-518/10, *Europska komisija protiv Republike Austrije*, 16. listopada 2012., st. 59. i 63.

203 CJEU, C-288/12, *Komisija protiv Mađarske,* 8. travnja 2012., odlomci 50 i 67.

Prema nacionalnom zakonodavstvu, nadzorna tijela imaju, među ostalim, sljedeće ovlasti i mogućnosti:[204]

- savjetovati nadzornike o svim pitanjima zaštite podataka
- istražiti postupke obrade i poduzeti mjere sukladno tome
- upozoriti ili opomenuti nadzornike
- naložiti ispravak, blokiranje, brisanje ili uništavanje podataka
- narediti privremenu ili konačnu zabranu obrade
- podnijeti slučaj sudu.

Kako bi moglo izvršavati svoje dužnosti, nadzorno tijelo mora imati pristup svim osobnim podacima i informacijama nužnim za istragu, kao i pristup svim prostorijama u kojima nadzornik čuva odgovarajuće informacije.

Postoje značajne razlike između domaćih nadležnosti koje se odnose na postupke i pravnog učinka nalaza nadzornog tijela. Mogu varirati od preporuka sličnih onima koje izdaje ombudsman do trenutačno provedivih odluka. Analizirajući učinkovitost pravnih lijekova dostupnih unutar nadležnosti, instrumente pravnih lijekova treba dakle procijeniti u njihovu kontekstu.

5.3. Pravni lijekovi i sankcije

Ključne točke

- Prema Konvenciji br. 108 i Direktivi o zaštiti podataka, nacionalnim se zakonodavstvom moraju utvrditi odgovarajući pravni lijekovi i sankcije za kršenje prava na zaštitu podataka.
    - Prema pravu Europske unije, za pravo na učinkovit pravni lijek potrebno je da se nacionalnim zakonodavstvom utvrde pravni lijekovi za kršenje prava na zaštitu podataka, neovisno o mogućnosti obraćanja nadzornom tijelu.

204 Direktiva o zaštiti podataka, članak 28.; vidjeti također Konvenciju br. 108, Dodatni protokol, čl. 1.

- Nacionalno zakonodavstvo mora propisati učinkovite, jednake, razmjerne i odvraćajuće sankcije.

- Prije nego što se obrati sudu, osoba se treba obratiti nadzorniku. Pitanje treba li se prije obraćanja sudu najprije obratiti nadzornom tijelu ostavljeno je na prosudbu nacionalnom zakonodavstvu.

- Osobe čiji se podaci obrađuju mogu podnijeti prijave o kršenju zakonodavstva o zaštiti podataka Europskom sudu za ljudska prava, no samo u krajnjoj nuždi i pod određenim uvjetima.

- Osim toga, osobe čiji se podaci obrađuju mogu se obratiti i Sudu Europske unije, ali samo u vrlo ograničenom broju slučajeva.

Prava na temelju zakonodavstva o zaštiti podataka može ostvariti samo ona osoba čija su prava ugrožena; to je osoba koja jest, ili bar tvrdi da jest, osoba čiji se podaci obrađuju. Te osobe u ostvarivanju prava mogu zastupati osobe koje, prema nacionalnom zakonodavstvu, ispunjavaju potrebne zahtjeve. Maloljetnike zastupaju njihovi roditelji ili skrbnici. Osobu pred nadzornim tijelima mogu zastupati i udruženja čiji je zakoniti cilj promicanje prava na zaštitu podataka.

5.3.1. Zahtjevi nadzorniku

Prava spomenuta u odjeljak 3.2 moraju se prvo ostvariti spram nadzornika. Izravno obraćanje nacionalnom nadzornom tijelu ili sudu ne bi pomoglo jer bi tijelo moglo osobu samo uputiti da se prvo obrati nadzorniku, a sud bi utvrdio da je predstavka neprihvatljiva. Službene zahtjeve za pravno relevantnim zahtjevom nadzorniku, naročito u pogledu toga trebaju li biti u pisanom obliku, treba urediti nacionalnim zakonodavstvom.

Na zahtjev odgovara tijelo kojemu se osoba obratila kao nadzorniku, čak i ako ono nije nadzornik. Odgovor se u svakom slučaju dostavlja osobi čiji se podaci obrađuju u vremenskom roku koji je utvrđen nacionalnim zakonodavstvom, čak i ako se u odgovoru navodi samo da se o podnositelju zahtjeva ne obrađuju nikakvi podaci. U skladu s odredbama članka 12. točke (a) Direktive o zaštiti podataka i članka 8. točke (b) Konvencije br. 108 taj se zahtjev treba obraditi „bez pretjeranog odgađanja." Stoga bi nacionalnim zakonodavstvom trebalo propisati dovoljno kratko razdoblje za odgovor, koje nadzorniku ipak omogućuje da na odgovarajući način obradi zahtjev.

Prije odgovaranja na zahtjev, tijelo kojemu se podnositelj zahtjeva obratio kao nadzorniku mora utvrditi identitet podnositelja zahtjeva kako bi bilo sigurno da je on

doista osoba koja tvrdi da jest i na taj način izbjeglo ozbiljno kršenje povjerljivosti. Ako zahtjevi za utvrđivanjem identiteta nisu posebno uređeni nacionalnim zakonodavstvom, o njima odlučuje nadzornik. Međutim, prema načelu poštene obrade, nadzornici ne bi smjeli propisivati pretjerano teške uvjete za potvrđivanje identifikacije (i autentičnosti zahtjeva, kako se razmatra u odjeljak 2.1.1).

Nacionalno se zakonodavstvo također treba baviti pitanjem smiju li nadzornici, prije nego što odgovore na zahtjev, tražiti da podnositelj zahtjeva plati naknadu: u članku 12. točki (a) direktive i članku 8. točki (b) Konvencije br. 108 propisano je da odgovor na zahtjeve za pristupom treba dati „bez pretjeranog [...] troška." Nacionalnim je zakonodavstvom u mnogim europskim zemljama propisano da na zahtjeve koji se tiču zakonodavstva o zaštiti podataka treba odgovoriti besplatno ako to ne uzrokuje pretjeran i neuobičajen napor. S druge su strane i nadzornici zaštićeni nacionalnim zakonodavstvom protiv zlouporabe prava na dobivanje odgovora na zahtjev.

Ako osoba, institucija ili tijelo kojima se podnositelj zahtjeva obrati kao nadzorniku ne opovrgne da je nadzornik, u vremenskom roku koji propisuje nacionalno zakonodavstvo taj subjekt mora:

- pristupiti zahtjevu i osobu koja je podnijela zahtjev obavijestiti o načinu na koji je zahtjevu udovoljeno ili

- podnositelja zahtjeva obavijestiti o razlogu iz kojeg njegovom zahtjevu nije udovoljeno.

5.3.2. Zahtjevi podneseni nadzornom tijelu

Ako osoba koja je podnijela zahtjev za pristupom ili uložila prigovor nadzorniku ne primi pravovremeni i zadovoljavajući odgovor, može se obratiti nacionalnom nadzornom tijelu nadležnom za zaštitu podataka sa zahtjevom za pomoći. Tijekom postupka pred nadzornim tijelom treba razjasniti je li osoba, institucija ili tijelo kojoj se obratio podnositelj zahtjeva doista bila dužna reagirati na zahtjev i je li reakcija bila ispravna i dostatna. Nadzorno tijelo mora obavijestiti predmetnu osobu o ishodu postupka u okviru kojeg se obrađuje njezin zahtjev.[205] Pravni učinci ishoda postupka pred nacionalnim nadzornim tijelima ovise o nacionalnom zakonodavstvu: mogu li se odluke tijela pravno provesti, odnosno može li ih provesti službeno tijelo ili se

205 Direktiva o zaštiti podataka, čl. 28. st. 4.

potrebno žaliti sudu ako nadzornik ne poštuje odluke (mišljenje, opomenu, itd.) nadzornog tijela.

U slučaju da su institucije ili tijela Europske unije navodno prekršile prava na zaštitu podataka zajamčena člankom 16. Ugovora o funkcioniranju Europske unije, osoba čiji se podaci obrađuju može podnijeti pritužbu Europskom nadzorniku za zaštitu podataka,[206] neovisnom nadzornom tijelu za zaštitu podataka prema Uredbi o zaštiti podataka u institucijama Europske unije kojom se utvrđuju dužnosti i ovlasti Europskog nadzornika za zaštitu podataka. Ako Europski nadzornik za zaštitu podataka ne odgovori u roku od šest mjeseci, smatra se da je pritužba odbijena.

Mora postojati mogućnost podnošenja žalbe sudu protiv odluka nacionalnog nadzornog tijela. To se odnosi na osobu čiji se podaci obrađuju kao i na nadzornike koji su sudjelovali u postupku pred nadzornim tijelom.

Primjer: Službenik za informacije Ujedinjene Kraljevine izdao je 24. lipnja 2013. odluku u kojoj od policije Hertfordshirea traži prestanak korištenja sustava praćenja registracijskih oznaka koji smatra nezakonitim. Podaci prikupljeni kamerom pohranjeni su i u lokalnim policijskim bazama podataka i u centraliziranoj bazi podataka. Fotografije registracijskih oznaka čuvale su se dvije godine, a fotografije automobila 90 dana. Smatralo se da takva opsežna uporaba kamera i drugih vrsta nadzora nije bila razmjerna problemu koji se pokušavao riješiti.

5.3.3. Zahtjev podnesen sudu

Prema Direktivi o zaštiti podataka, ako osoba koja je nadzorniku podnijela zahtjev na temelju zakonodavstva o zaštiti podataka nije zadovoljna odgovorom nadzornika, mora imati pravo na podnošenje žalbe nacionalnom sudu.[207]

Pitanje treba li se prije obraćanja sudu najprije obratiti nadzornom tijelu ostavljeno je na prosudbu nacionalnom zakonodavstvu. Međutim, u većini se slučajeva osobama koje ostvaruju svoja prava na zaštitu podataka preporučuje da se prvo obrate nadzornom tijelu jer bi postupci zahtjeva za njihovom pomoći trebali biti nebirokratski i besplatni. Stručno znanje dokumentirano u odluci (mišljenju, opomeni, itd.)

206 Uredba (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka SL L 2001 L 8.

207 Direktiva o zaštiti podataka, čl. 22.

nadzornog tijela također može pomoći osobi čiji se podaci obrađuju u ostvarenju prava pred sudovima.

Unutar prava Vijeća Europe, kršenja prava na zaštitu podataka do kojih je navodno došlo na nacionalnoj razini ugovorne stranke Europske konvencije o ljudskim pravima i koja istovremeno predstavljaju kršenje članka 8. Europske konvencije o ljudskim pravima mogu se dodatno podnijeti Europskom sudu za ljudska prava nakon što se iscrpe svi dostupni domaći pravni lijekovi. Da bi se obratilo Europskom sudu za ljudska prava zbog kršenja članka 8. Europske konvencije o ljudskim pravima, također trebaju biti ispunjeni drugi kriteriji prihvatljivosti (članci 34. do 37. Europske konvencije o ljudskim pravima).[208]

Iako zahtjevi Europskom sudu za ljudska prava mogu biti usmjereni samo protiv ugovornih stranaka, neizravno se mogu baviti i postupcima ili propustima privatnih stranaka, pod uvjetom da ugovorna stranka nije ispunila svoje pozitivne obveze prema Europskoj konvenciji o ljudskim pravima niti osigurala dovoljnu zaštitu protiv kršenja prava na zaštitu podataka u svojem nacionalnom zakonodavstvu.

Primjer: U predmetu *K.U. protiv Finske*,[209] podnositelj, maloljetnik, žalio se da je o njemu objavljen oglas seksualne prirode na internetskoj stranici za upoznavanje. Davatelj usluge nije otkrio identitet osobe koja je objavila informacije zbog obveza povjerljivosti prema finskom zakonodavstvu. Podnositelj je tvrdio da finskim zakonodavstvom nije osigurana dostatna zaštita od takvih radnji privatne osobe koja je na internetu objavila inkriminirajuće podatke o podnositelju. Europski sud za ljudska prava smatrao je da su države bile dužne suzdržati se od proizvoljnog miješanja u privatne živote pojedinaca i da su mogle podlijegati pozitivnim obvezama koje uključuju „usvajanje mjera u cilju poštovanja privatnog života čak i u području uzajamnih odnosa pojedinaca." U slučaju podnositelja, da bi ga se praktično i učinkovito zaštitilo, valjalo je poduzeti učinkovite mjere identificiranja i progona počinitelja. Međutim, država nije osigurala takvu zaštitu te je Sud zaključio da je prekršen članak 8. Europske konvencije o ljudskim pravima.

208 Europska konvencija o ljudskim pravima, članci 34. - 37., dostupno na: www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.

209 *ECtHR, K.U. protiv Finske*, br. 2872/02, 2. ožujka 2009.

Primjer: U predmetu Köpke protiv Njemačke,[210] podnositeljica je osumnjičena za krađu na radnom mjestu te je podvrgnuta video nadzoru. Europski sud za ljudska prava zaključio je da „ništa ne upućuje na to da domaća nadležna tijela nisu uspostavila poštenu ravnotežu, prema vlastitoj procjeni, između prava podnositeljice na poštovanje njezina privatnog života prema članku 8. s jedne strane i interesa njezina poslodavca da zaštiti svoja vlasnička prava i javnog interesa za ispravnom primjenom pravde s druge strane." Stoga je zahtjev proglašen neprihvatljivim.

Ako Europski sud za ljudska prava utvrdi da je država stranka prekršila prava koja se štite Europskom konvencijom o ljudskim pravima, država stranka mora izvršiti presudu Europskog suda za ljudska prava. Izvršnim mjerama treba prvo zaustaviti kršenje i ispraviti, koliko je to moguće, negativne posljedice kršenja za podnositelja. Izvršenje presuda može iziskivati i opće mjere kojima se sprečavaju kršenja slična onima koje je utvrdio Sud, bilo unosom promjena u zakonodavstvo, sudsku praksu ili na drugi način.

Ako je Europski sud za ljudska prava utvrdio kršenje Europske konvencije o ljudskim pravima, njezinim člankom 41. propisano je da Sud može podnositelju dosuditi pravičnu naknadu o trošku države stranke.

Unutar prava Europske unije,[211] žrtve kršenja nacionalnog zakonodavstva o zaštiti podataka, kojime se provodi zakonodavstvo Europske unije o zaštiti podataka, u određenim okolnostima mogu svoje predmete podnijeti Sudu Europske unije. Tužba osobe čiji se podaci obrađuju zbog kršenja prava na zaštitu podataka može imati za ishod postupak pred Sudom Europske unije. Dva su moguća scenarija za to.

U prvom bi scenariju osoba čiji se podaci obrađuju trebala biti izravna žrtva upravnog ili regulatornog akta Europske unije kojime su prekršena prava pojedinca na zaštitu podataka. Prema članku 263. stavku 4. Ugovora o funkcioniranju Europske unije:

> *„svaka fizička ili pravna osoba može [...] pokrenuti postupak protiv akta koji je upućen toj osobi ili koji se izravno i osobno odnosi na nju te protiv regulatornog akta koji se izravno odnosi na nju, a ne podrazumijeva provedbene mjere."*

210 ECtHR, *Köpke protiv Njemačke* (dec.), br. 420/07, 5. listopada 2010.

211 EU (2007), Ugovor iz Lisabona o izmjenama Ugovora o Europskoj uniji i Ugovora o osnivanju Europske zajednice, potpisan u Lisabonu 13. prosinca 2007., SL 306. Vidjeti također pročišćene verzije Ugovora o Europskoj uniji, SL 2012 C 326 i Ugovora o funkcioniranju Europske unije, SL L 2012 C 326.

Stoga se žrtve nezakonite obrade podataka koju je provelo tijelo Europske unije mogu žaliti izravno Općem sudu Suda Europske unije, tijelu nadležnom za donošenje presuda u predmetima koji se tiču Uredbe o zaštiti podataka u institucijama Europske unije. Mogućnost izravne žalbe Sudu Europske unije postoji i ako zakonska odredba Europske unije izravno utječe na pravnu situaciju pojedinca.

Drugi se scenarij odnosi na nadležnost Suda Europske unije (Sud) vezanu uz donošenje prethodnih odluka prema članku 267. Ugovora o funkcioniranju Europske unije.

U fazi odvijanja domaćeg postupka, osobe čiji se podaci obrađuju mogu od nacionalnog suda zatražiti da zahtijeva objašnjenje od Suda o tumačenju Ugovora o Europskoj uniji i o tumačenju valjanosti akata institucija, tijela, ureda ili agencija Europske unije. Takva se objašnjenja nazivaju prethodnim odlukama. To nije izravni lijek za podnositelja, ali nacionalnim sudovima omogućuje primjenu točnog tumačenja prava Europske unije.

Ako stranka u postupku pred nacionalnim sudovima zatraži upućivanje pitanja Sudu Europske unije, zahtjevu su obvezni udovoljiti samo nacionalni sudovi koji djeluju kao zadnja sudska instanca i protiv čijih odluka ne postoji pravni lijek.

Primjer: U predmetu *Kärntner Landesregierung i drugi*,[212] austrijski Ustavni sud podnio je pitanja Sudu Europske unije u vezi s valjanošću članaka 3. do 9. Direktive 2006/24/EZ (*Direktiva o zadržavanju podataka*) u svjetlu članaka 7., 9. i 11. Povelje. Pitanje se odnosilo i na to jesu li određene odredbe austrijskog Saveznog zakona o telekomunikacijama kojima se prenosi Direktiva o zadržavanju podataka nespojive s aspektima Direktive o zaštiti podataka i Uredbe o zaštiti podataka u institucijama Europske unije.

G. Seitlinger, jedan od podnositelja u postupcima Ustavnog suda, tvrdio je da telefon, internet i e-poštu koristi i u poslovne i u privatne svrhe. Sukladno tome, informacije koje šalje i prima prolaze kroz javne telekomunikacijske mreže. Prema austrijskom Zakonu o telekomunikacijama iz 2003., njegov davatelj telekomunikacijskih usluga zakonski je obvezan prikupljati i pohranjivati podatke o njegovoj uporabi mreže. G. Seitlinger je shvatio da davatelj telekomunikacijskih usluga nije nužno morao prikupljati i pohranjivati njegove osobne podatke u tehničke svrhe slanja informacija od točke A do točke B unutar mreže. Osim toga, prikupljanje i pohrana tih podataka nisu nikako bili nužni u svrhu naplate.

212 CJEU, zajednički predmeti C-293/13 i C-594/12, *Digital Rights Ireland i Seitling i drugi*, 8. travnja 2014.

G. Seitlinger zasigurno nije pristao na takvu uporabu svojih osobnih podataka. Jedini razlog za prikupljanje i pohranu svih tih dodatnih podataka bio je austrijski Zakon o telekomunikacijama iz 2003.

Stoga je g. Seitlinger pred austrijskim Ustavnim sudom pokrenuo postupak u kojemu je tvrdio da statutarne obveze njegovog davatelja telekomunikacijskih usluga krše njegova temeljna prava prema članku 8. Povelje Europske unije.

Sud Europske unije donosi odluke samo o sastavnim dijelovima zahtjeva za prethodnom odlukom koji mu je podnesen. Nacionalni sud ostaje nadležan za odlučivanje o izvornom slučaju.

Sud u načelu mora odgovoriti na postavljena pitanja. Ne može odbiti donošenje prethodne odluke zbog toga što taj odgovor ne bi bio ni relevantan ni pravovremen u pogledu izvornog slučaja. Međutim, može odbiti donošenje prethodne odluke ako pitanje nije unutar njegovog područja nadležnosti.

Konačno, ako prava na zaštitu podataka, zajamčena člankom 16. Ugovora o funkcioniranju Europske unije, navodno prekrši institucija ili tijelo Europske unije tijekom obrade osobnih podataka, osoba čiji se podaci obrađuju može slučaj podnijeti Općem sudu Suda Europske unije (članak 32. stavci 1. i 4. Uredbe o zaštiti podataka u institucijama Europske unije). Isto se odnosi na odluke Europskog nadzornika za zaštitu podataka u vezi s takvim kršenjima (članak 32. stavak 3. Uredbe o zaštiti podataka u institucijama Europske unije).

Opći sud Suda Europske unije nadležan je za donošenje odluka u predmetima koji se tiču Uredbe o zaštiti podataka u institucijama Europske unije. No, ako osoba u svojstvu člana osoblja institucije ili tijela Europske unije zatraži pravni lijek, mora se obratiti Službeničkom sudu Europske unije.

Primjer: Predmet *Europska komisija protiv The Bavarian Lager Co. Ltd*[213] ukazuje na pravne lijekove koji se mogu primijeniti protiv aktivnosti ili odluka institucija i tijela Europske unije u vezi sa zaštitom podataka.

Bavarian Lager je od Europske komisije zatražio pristup cjelokupnom zapisniku sa sastanka koji je održala Komisija a koji se navodno odnosio na pravna pitanja

213 CJEU, C-28/08 P, *Europska komisija protiv The Bavarian Lager Co. Ltd*, 29. lipnja 2010.

bitna za društvo. Komisija je odbila zahtjev društva iz razloga prevladavajućih interesa zaštite podataka.[214] Pozivajući se na članak 32. Uredbe o zaštiti podataka u institucijama Europske unije, Bavarian Lager je protiv te odluke uložio žalbu Sudu Europske unije; točnije, Prvostupanjskom sudu (prethodnik Općeg suda). U svojoj odluci u predmetu T-194/04, *Bavarian Lager protiv Komisije,* Prvostupanjski sud poništio je odluku Komisije kojom je odbijen zahtjev za pristupom. Europska komisija žalila se na tu odluku Sudu Europske unije. Veliko vijeće Suda donijelo je presudu kojom je odbačena presuda Prvostupanjskog suda i potvrđeno odbacivanje zahtjeva za pristupom Europske komisije.

5.3.4. Sankcije

Unutar prava Vijeća Europe, člankom 10. Konvencije br. 108 propisano je da svaka stranka mora uspostaviti odgovarajuće sankcije i pravne lijekove za kršenja odredbi domaćeg zakonodavstva kojima se provode osnovna načela zaštite podataka navedena u Konvenciji br. 108.[215] **Unutar prava Europske unije**, člankom 24. Direktive o zaštiti podataka propisano je da „države članice donose odgovarajuće mjere kako bi osigurale potpunu provedbu odredbi ove Direktive i posebno propisuju sankcije koje se nameću u slučaju kršenja odredbi donesenih […]."

Oba instrumenta državama članicama omogućuju veliku slobodu odabira odgovarajućih sankcija i pravnih lijekova. Nijedan pravni instrument ne nudi konkretne smjernice u vezi s načinom ili vrstom odgovarajućih sankcija niti navodi primjere sankcija.

Međutim:

> *„iako države članice Europske unije uživaju veliku slobodu odlučivanja o mjerama koje su najprikladnije za zaštitu prava pojedinaca na temelju prava Europske unije, u skladu s načelom lojalne suradnje kako je navedena u članku 4. stavku 3. Ugovora o Europskoj uniji, valja ispuniti minimalne zahtjeve u pogledu učinkovitosti, jednakosti, razmjernosti i odvraćanja."*[216]

214 Za analizu argumenata vidjeti: EDPS (2011), *Javni pristup dokumentima koji sadrže osobne podatke nakon odluke o predmetu* Bavarian Lager, Bruxelles, Europski nadzornik za zaštitu podataka, dostupno na: www.secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

215 ECtHR, *I. protiv Finske*, br. 20511/03, 17. srpnja 2008.; ECtHR, *K.U. protiv Finske*, br. 2872/02, 2. prosinca 2008.

216 FRA (2012), *Mišljenje Agencije Europske unije za temeljna prava o predloženom paketu reformi zaštite podataka*, 2/2012, Beč, 1. listopada 2012., str. 27.

Sud Europske unije u više je navrata tvrdio da nacionalno zakonodavstvo nema potpunu slobodu određivanja sankcija.

> Primjer: U predmetu *Von Colson i Kamann protiv Land Nordrhein-Westfalen,*[217] Sud Europske unije istaknuo je da su sve države članice na koje se odnosi Direktiva u svojim nacionalnim pravnim sustavima dužne usvojiti sve potrebne mjere kojima se osigurava njezina učinkovitost u skladu s njezinim ciljem. Sud je smatrao da, iako države članice odabiru načine i sredstva kojima osiguravaju provedbu Direktive, ta sloboda ne utječe na obvezu kojoj podliježu. Točnije, učinkovit pravni lijek mora pojedincu omogućiti potpuno ostvarenje i provedbu predmetnog prava. Kako bi se osigurala takva prava i učinkovita zaštita, pravni lijekovi moraju dovesti do kaznenih i/ili kompenzacijskih postupaka čiji su ishod sankcije s odvraćajućim učinkom.

Što se tiče sankcija protiv kršenja prava Europske unije od strane institucija ili tijela Europske unije, zbog posebne ovlasti Uredbe o zaštiti podataka u institucijama Europske unije, sankcije su predviđene samo u obliku disciplinskih mjera. Prema članku 49. Uredbe, „zbog neizvršavanja obveza iz ove Uredbe, bilo namjerno ili zbog nemara, dužnosnik ili drugi službenik Europskih zajednica bit će podvrgnut disciplinskoj mjeri […].”

217 CJEU, C-14/83, *Sabine von Kolson i Elisabeth Kamann protiv Pokrajine Sjeverne Rajne – Vestfalije,* 10. travnja 1984.

6 Prekogranični prijenosi podataka

EU	Pitanja kojima se bavi	Vijeće Europe
Prekogranični prijenosi podataka		
Direktiva o zaštiti podataka, članak 25. stavak 1. CJEU, C-101/01, *Bodil Lindqvist*, 6. studenoga 2003.	**Definicija**	Konvencija br. 108, Dodatni protokol, članak 2. stavak 1.
Slobodan prijenos podataka		
Direktiva o zaštiti podataka, članak 1. stavak 2.	**Među državama članicama Europske unije**	
	Među ugovornim strankama Konvencije br. 108	Konvencija br. 108, članak 12. stavak 2.
Direktiva o zaštiti podataka, članak 25.	**Trećim zemljama s odgovarajućom razinom zaštite podataka**	Konvencija br. 108, Dodatni protokol, članak 2. stavak 1.
Direktiva o zaštiti podataka, članak 26. stavak 1.	**Trećim zemljama u posebnim slučajevima**	Konvencija br. 108, Dodatni protokol, članak 2. stavak 2. točka (a)
Ograničeni prijenos podataka trećim zemljama		
Direktiva o zaštiti podataka, članak 26. stavak 2. Direktiva o zaštiti podataka, članak 26. stavak 4.	**Ugovorne klauzule**	Konvencija br. 108, Dodatni protokol, članak 2. stavak 2. točka (b) Vodič za pripremu ugovornih klauzula
Direktiva o zaštiti podataka, članak 26. stavak 2.	**Obvezujuća pravila poduzeća**	

EU	Pitanja kojima se bavi	Vijeće Europe
Primjeri: Sporazum između Europske unije i SAD-a o PNR-u Sporazum između Europske unije i SAD-a o SWIFT-u	Posebni međunarodni sporazumi	

Osim što je u Direktivi o zaštiti podataka propisan slobodan prijenos podataka među državama članicama, ona sadrži i odredbe o zahtjevima za prijenos osobnih podataka trećim zemljama izvan Europske unije. Vijeće Europe prepoznalo je i važnost provedbenih pravila za prekogranični prijenos podataka trećim zemljama te 2001. godine usvojilo Dodatni protokol uz Konvenciju br. 108. Tim su Protokolom preuzete glavne regulatorne značajke prekograničnog prijenosa podataka iz država stranaka konvencije i članica Europske unije.

6.1. Narav prekograničnog prijenosa podataka

Ključne točke

- Prekogranični prijenos podataka je prijenos osobnih podataka primatelju koji je pod stranom nadležnosti.

U članku 2. stavku 1. Dodatnog protokola uz Konvenciju br. 108 prekogranični prijenos podataka opisuje se kao prijenos osobnih podataka primatelju koji je pod stranom nadležnosti. Člankom 25. stavkom 1. Direktive o zaštiti podataka uređuje se „prijenos trećoj zemlji osobnih podataka koji se obrađuju ili koje je potrebno obraditi nakon prijenosa [...].” Takav je prijenos podataka dopušten samo u skladu s pravilima navedenim u članku 2. Dodatnog protokola uz Konvenciju br. 108 te, za države članice Europske unije, dodatno u člancima 25. i 26. Direktive o zaštiti podataka.

Primjer: U predmetu *Bodil Lindqvist*,[218] Sud Europske unije smatrao je da se „upućivanje na različite osobe na internetskoj stranici te njihovo identificiranje imenom ili na drugi način, primjerice navođenjem njihova telefonskog broja ili

218 CJEU, C-101/01, *Bodil Lindqvist*, 6. studenoga 2003. 27., 68. i 69.

informacija u vezi njihovih radnih uvjeta ili hobija, smatra 'osobnim podacima koji se u cijelosti ili djelomično obrađuju automatskim putem' u smislu članka 3. stavka 1. Direktive 95/46."

Sud je zatim istaknuo da se Direktivom također propisuju posebna pravila čiji je cilj omogućiti državama članicama nadzor prijenosa osobnih podataka trećim zemljama.

Međutim, s obzirom na, u prvom redu, stanje razvijenosti interneta u trenutku sastavljanja Direktive, a zatim i na njen nedostatak kriterija koji se odnose na uporabu interneta, „ne može se pretpostaviti da je zakonodavac Zajednice namjeravao da izraz „prijenos [podataka] trećoj zemlji" pokriva učitavanje [podataka] na internetsku stranicu, čak i ako na taj način podaci postanu dostupni osobama u trećim zemljama koje imaju tehnička sredstva da im pristupe."

Kada bi se Direktiva „tumačila na način da do prijenosa podataka trećoj zemlji dolazi svaki put kad se osobni podaci učitaju na internetsku stranicu, taj bi prijenos nužno bio prijenos svim trećim zemljama u kojima postoje tehnička sredstva potrebna za pristup internetu. Na taj bi način poseban režim koji je propisan [Direktivom] nužno postao režim opće primjene, u pogledu aktivnosti na internetu. Ako bi Komisija dakle utvrdila [...] da čak i samo jedna treća zemlja nije osigurala dovoljnu zaštitu, države članice bile bi dužne onemogućiti stavljanje osobnih podataka na internet."

Načelo da se puka objava (osobnih) podataka ne treba smatrati prekograničnim prijenosom podataka odnosi se i na on-line javne registre ili sredstva javnog priopćavanja kao što su (elektroničke) novine i televizija. Pojam „prekograničnog prijenosa podataka" odnosi se samo na komunikaciju koja je usmjerena na određene primatelje.

6.2. Slobodan protok podataka među državama članicama ili među ugovornim strankama

Ključne točke

- Prijenos osobnih podataka drugoj državi članici Europskog gospodarskog prostora ili drugoj ugovornoj stranki Konvencije br. 108 ne smije se ograničavati.

Prema članku 12. točki (c) Konvencije br. 108, **unutar prava Vijeća Europe** mora postojati slobodan prijenos osobnih podataka među strankama konvencije. Domaćim se zakonodavstvom ne smije ograničiti izvoz osobnih podataka ugovornim strankama, osim:

- ako je to nužno zbog posebne naravi podataka[219]
- ako je ograničenje nužno kako bi se spriječilo izbjegavanje nacionalnih zakonskih odredbi o prekograničnom prijenosu podataka trećim zemljama.[220]

Unutar prava Europske unije, ograničenja ili zabrane slobodnog prijenosa podataka među državama članicama zbog zaštite podataka zabranjena su člankom 1. stavkom 2. Direktive o zaštiti podataka. Područje slobodnog prijenosa podataka prošireno je Ugovorom o europskom gospodarskom prostoru (EGP),[221] kojime se Island, Lihtenštajn i Norveška uvode na unutarnje tržište.

Primjer: Ako podružnica međunarodne grupacije s poslovnim nastanom u nekoliko država članica Unije, među ostalim u Sloveniji i Francuskoj, prenosi osobne podatke iz Slovenije u Francusku, takav se prijenos podataka ne smije ograničiti niti zabraniti slovenskim nacionalnim zakonodavstvom.

Međutim, ako ista slovenska podružnica želi prenijeti iste te osobne podatke matičnom društvu u Sjedinjenim Američkim Državama, slovenski izvoznik podataka mora proći postupak propisan slovenskim zakonodavstvom o prekograničnom prijenosu podataka trećim zemljama bez odgovarajuće zaštite podataka, osim ako je matično društvo usvojilo načela privatnosti sigurne luke, dobrovoljni kodeks ponašanja o osiguravanju odgovarajuće razine zaštite podataka (vidjeti odjeljak 6.3.1).

Međutim, prekogranični prijenosi podataka državama članicama EGP-a u svrhe izvan nadležnosti unutarnjeg tržišta, kao što je istraga zločina, ne podliježu odredbama Direktive o zaštiti podataka pa se na njih ne može odnositi načelo slobodnog prijenosa podataka. Što se tiče prava Vijeća Europe, sva su područja uključena u opseg

219 Konvencija br. 108, čl. 12. stavak 3. točka (a).

220 *Ibid.*, čl. 12. st. 3. točka (b).

221 Odluka Vijeća i Komisije od 13. prosinca 1993. o sklapanju Ugovora o europskom gospodarskom prostoru između Europskih zajednica, njihovih država članica i Republike Austrije, Republike Finske, Republike Island, Kneževine Lihtenštajna, Kraljevine Norveške, Kraljevine Švedske i Švicarske Konfederacije, SL 1994 L 1.

primjene Konvencije br. 108 i Dodatnog protokola uz Konvenciju br. 108, s time da ugovorne stranke mogu utvrditi izuzeća. Svi članovi EGP-a također su stranke Konvencije br. 108.

6.3. Slobodan prijenos podataka trećim zemljama

Ključne točke

- Prijenos osobnih podataka trećim zemljama mora biti lišen ograničenja prema nacionalnom zakonodavstvu o zaštiti podataka ako:
  - je potvrđena odgovarajuća zaštita podataka kod primatelja
  - je to nužno radi posebnih interesa osobe čiji se podaci obrađuju ili zakonitih prevladavajućih interesa drugih, naročito važnih javnih interesa.
- Odgovarajuća zaštita podataka u trećoj zemlji znači da su glavna načela zaštite podataka učinkovito provedena u nacionalnom zakonodavstvu te zemlje.
- Unutar prava Europske unije, Europska komisija procjenjuje prikladnost zaštite podataka u trećoj zemlji. Unutar prava Vijeća Europe, na nacionalnom je zakonodavstvu da utvrdi način na koji će procijeniti prikladnost zaštite podataka.

6.3.1. Slobodan prijenos podataka radi prikladne zaštite

Prema **pravu Vijeća Europe**, nacionalnim se zakonodavstvom može dopustiti slobodan prijenos podataka državama koje nisu stranke ugovora ako država ili organizacija primatelj osiguravaju dovoljnu razinu zaštite podataka koji se planiraju prenijeti.[222] Nacionalnim se zakonodavstvom utvrđuje način procjene razine zaštite podataka u stranoj zemlji i tko bi procjenu trebao izvršiti.

Unutar prava Europske unije, slobodan prijenos podataka trećim zemljama s odgovarajućom razinom zaštite podataka propisan je člankom 25. stavkom 1. Direktive o zaštiti podataka. Zbog uvjeta koji umjesto jednakosti prednost daje prikladnosti, postoje različiti načini provedbe zaštite podataka. Prema članku 25. stavku 6.

222 Konvencija br. 108, Dodatni protokol, čl. 2. st. 1.

Direktive, Europska komisija nadležna je procijeniti razinu zaštite podataka u stranim zemljama na temelju zaključaka o prikladnosti. Ona se savjetuje o procjeni s Radnom skupinom iz članka 29. koja je značajno doprinijela tumačenju članaka 25. i 26.[223]

Zaključak Europske komisije o prikladnosti ima obvezujući učinak. Ako Europska komisija objavi zaključak o prikladnosti za određenu zemlju u *Službenom listu Europske unije*, sve zemlje članice EGP-a i njihova tijela dužni su poštovati odluku. To znači da se podaci mogu prenositi u tu zemlju bez postupaka provjere ili licenciranja pred nacionalnim tijelima.[224]

Europska komisija također može procijeniti dijelove pravnog sustava zemlje ili se ograničiti na pojedinačne teme. Komisija je donijela zaključak o prikladnosti, na primjer, samo o kanadskom zakonodavstvu o privatnim trgovačkim društvima.[225] Niz je zaključaka o prikladnosti za prijenose koji se temelje na ugovorima između Europske unije i stranih zemalja. Te se odluke odnose isključivo na jednu vrstu prijenosa podataka, kao što su evidencije imena putnika koji zračne kompanije prenose stranim tijelima za graničnu kontrolu kad zrakoplov leti iz Europske unije u određena prekomorska odredišta (vidjeti odjeljak 6.4.3). U novijoj se praksi prijenosa podataka na temelju posebnih ugovora između Europske unije i trećih zemalja općenito ne koriste zaključci o prikladnosti jer se pretpostavlja da se samim ugovorom osigurava odgovarajuća razina zaštite podataka.[226]

Jedna od najvažnijih odluka o prikladnosti zapravo se ne odnosi na skup pravnih odredbi.[227] Odnosi se na pravila, uvelike slična Kodeksu ponašanja, poznata kao

223 Vidjeti, na primjer, Radnu skupinu iz članka 29. (2003), *Radni dokument o prijenosima osobnih podataka trećim zemljama: primjena članka 26. stavka 2. Direktive Europske unije o zaštiti podataka na obvezujuća pravila poduzeća za međunarodne prijenose podataka,* WP 74, Bruxelles, 3. lipnja 2003.; i Radnu skupinu iz članka 29. (2005), *Radni dokument o zajedničkom tumačenju članka 26. stavka 1. Direktive 95/46/EZ od 24. listopada 1995.*, WP 144, Bruxelles, 25. studenoga 2005.

224 Za najnoviju verziju popisa zemalja koje su primile zaključak o prikladnosti vidjeti početnu stranicu Europske komisije, Glavnu upravu za pravosuđe, na adresi: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

225 Europska Komisija (2002), Odluka 2002/2/EZ od 20. prosinca 2001. u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća o odgovarajućoj zaštiti osobnih podataka propisanoj kanadskim Zakonom o zaštiti osobnih podataka i elektroničkih dokumenata, SL 2002 L 2.

226 Na primjer, Sporazum između Sjedinjenih Američkih Država i Europske unije o uporabi i prijenosu Evidencije imena putnika Ministarstvu domovinske sigurnosti Sjedinjenih Američkih Država (SL 2012 L 215, st. 5.–14.) ili Sporazum između Europske unije i Sjedinjenih Američkih Država o obradi i prijenosu podataka o financijskim porukama koje se iz Europske unije šalju Sjedinjenim Američkim Državama u svrhu Programa praćenja financiranja terorističkih aktivnosti, SL 2010 L 8, str. 11.–16.

227 Europska komisija (2000), Odluka Komisije 2000/520/EZ od 26. srpnja 2006. u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća o prikladnosti zaštite koju pružaju načela privatnosti sigurne luke i uz njih vezana često postavljana pitanja koje je izdalo Ministarstvo trgovine SAD-a SL L 2000 L 215.

načela privatnosti sigurne luke. Ta su načela razradile Europska unija i Sjedinjene Američke Države za trgovačka društva SAD-a. Članstvo u sigurnoj luci ostvaruje se dobrovoljnim preuzimanjem obveze pred Ministarstvom trgovine SAD-a koje se dokumentira na popisu koji izdaje to ministarstvo. Budući da je jedan od bitnih elemenata prikladnosti učinkovitost provedbe zaštite podataka, dogovorom o sigurnoj luci otvara se i određena razina nadzora od strane države: sigurnoj luci mogu pristupiti samo one države koje podliježu nadzoru Savezne trgovinske komisije SAD-a.

6.3.2. Slobodan prijenos podataka u posebnim slučajevima

Unutar prava Vijeća Europe, člankom 2. stavkom 2. Dodatnog protokola uz Konvenciju br. 108 omogućen je prijenos osobnih podataka trećim zemljama u kojima nema prikladne zaštite podataka, pod uvjetom da je prijenos propisan nacionalnim zakonodavstvom i nužan zbog:

- posebnih interesa osobe čiji se podaci obrađuju
- zakonitih prevladavajućih interesa drugih, posebno važnih javnih interesa.

Unutar prava Europske unije, u članku 26. stavku 1. Direktive o zaštiti podataka sadržane su odredbe slične onima iz Dodatnog protokola uz Konvenciju br. 108.

Prema Direktivi, interesi osobe čiji se podaci obrađuju mogu opravdati slobodan prijenos podataka trećoj zemlji ako:

- osoba čiji se podaci obrađuju da svoju nedvosmislenu suglasnost za izvoz podataka
- osoba čiji se podaci obrađuju sklopi, ili se priprema sklopiti, ugovorni odnos čiji je izričiti preduvjet prijenos podataka primatelju u inozemstvu
- su nadzornik i treća stranka sklopili ugovor u interesu osobe čiji se podaci obrađuju
- ako je prijenos potreban kako bi se zaštitili vitalni interesi osobe čiji se podaci obrađuju

- za prijenos podataka iz javnih registara; radi se o prevladavajućim interesima javnosti koji se tiču pristupa informacijama pohranjenim u javnim registrima.

Zakoniti interesi drugih mogu opravdati slobodan prekogranični prijenos podataka:[228]

- radi važnog javnog interesa, osim pitanja nacionalne ili javne sigurnosti, jer ona nisu obuhvaćena Direktivom o zaštiti podataka

- radi uspostave, izvršenja ili obrane pravnih zahtjeva.

Gore navedene slučajeve treba shvatiti kao izuzeća od pravila koje glasi da je za neometani prijenos podataka drugim zemljama potrebna odgovarajuća razina zaštite podataka u zemlji primateljici. Izuzeća treba uvijek tumačiti restriktivno. To je u više navrata isticala Radna skupina iz članka 29. u kontekstu članka 26. stavka 1. Direktive o zaštiti podataka, naročito ako je suglasnost navodna osnova za prijenos podataka.[229] Radna skupina iz članka 29. zaključila je da se opća pravila o pravnom značaju suglasnosti odnose i na članak 26. stavak 1. Direktive. Ako, na primjer, u kontekstu radnih odnosa, nije jasno je li suglasnost koju su dali zaposlenici doista slobodna suglasnost, prijenosi podataka ne mogu se temeljiti na članku 26. stavku 1. točki (a) Direktive. U tim se slučajevima primjenjuje članak 26. stavak 2. koji propisuje da nacionalna tijela za zaštitu podataka izdaju dozvolu za prijenose podataka.

6.4. Ograničeni prijenos podataka trećim zemljama

Ključne točke

- Prije izvoza podataka trećim zemljama u kojima nije osigurana odgovarajuća razina zaštite podataka, nadzorno tijelo može zatražiti od nadzornika da mu omogući uvid u podatke koje namjerava iznositi.
- Nadzornik koji želi izvesti podatke mora dokazati dvije stvari tijekom tog pregleda:
  - da postoji pravna osnova za prijenos podataka primatelju

228 Direktiva o zaštiti podataka, čl. 26. st. 1. točka (d).

229 Vidjeti naročito Radnu skupinu iz članka 29. (2005), *Radni dokument o zajedničkom tumačenju članka 26. stavka 1. Direktive 95/46/EZ od 24. listopada 1995.*, WP 144, Bruxelles, 25. studenoga 2005.

  - da se provode mjere za zaštitu odgovarajuće zaštite podataka kod primatelja.
- Mjere za uspostavu odgovarajuće zaštite podataka kod primatelja mogu uključivati:
  - ugovorne odredbe između nadzornika koji izvozi podatke i stranog primatelja podataka ili
  - obvezujuća pravila poduzeća koja se obično odnose na prijenose podataka unutar multinacionalne grupacije.
- Prijenosi podataka stranim tijelima mogu se urediti i posebnim međunarodnim sporazumom.

Sukladno Direktivi o zaštiti podataka i Dodatnom protokolu uz Konvenciju br. 108 nacionalno zakonodavstvo može uspostaviti režime za prekogranične prijenose podataka trećim zemljama u kojima nije osigurana odgovarajuća razina zaštite podataka pod uvjetom da je nadzornik poduzeo posebne radnje kojima se osiguravaju odgovarajuće mjere zaštite podataka kod primatelja i pod uvjetom da nadzornik može to dokazati nadležnom tijelu. Taj je zahtjev izričito naveden samo u Dodatnom protokolu uz Konvenciju br. 108; međutim, smatra se standardnim postupkom i prema Direktivi o zaštiti podataka.

6.4.1. Ugovorne klauzule

I u **pravu Vijeća Europe** i u **pravu Europske unije** spominju se ugovorne klauzule kojima se vezuju nadzornik koji izvozi podatke i primatelj u trećoj zemlji. Takve klauzule navode se kao mogući način osiguravanja odgovarajuće razine zaštite podataka kod primatelja.

Na **razini Europske unije**, Europska komisija uz pomoć Radne skupine iz članka 29. razvila je standardne ugovorne klauzule koje su službeno ovjerene Odlukom Komisije kao dokaz odgovarajuće razine zaštite podataka.[230] S obzirom na to da su odluke Komisije u cijelosti obvezujuće u državama članicama, nacionalna tijela odgovorna za nadzor prekograničnog prijenosa podataka moraju potvrditi te standardne ugovorne klauzule u svojim postupcima.[231] Stoga, ako se nadzornik i primatelj iz treće zemlje dogovore i potpišu ih, to bi za nadzorno tijelo trebao biti dovoljan dokaz provođenja odgovarajućih zaštitnih mjera.

230 Direktiva o zaštiti podataka, čl. 26. st. 4.

231 Ugovor o funkcioniranju Europske unije, čl. 288.

Postojanje standardnih ugovornih klauzula u pravnom okviru Europske unije ne znači da nadzornici ne smiju sastavljati druge *ad hoc* ugovorne klauzule. Međutim, tim bi klauzulama trebali osigurati jednaku razinu zaštite koju osiguravaju standardne ugovorne klauzule. Najvažnije značajke standardnih ugovornih klauzula jesu:

- odredba o korisniku trećoj stranci kojom se osobama čiji se podaci obrađuju omogućuje ostvarivanje ugovornih prava iako nisu stranke ugovora

- primatelj ili uvoznik podataka pristaje na podvrgavanje postupku nacionalnog nadzornog tijela i/ili sudova nadzornika koji izvozi podatke u slučaju spora.

Dostupne su dvije skupine standardnih klauzula za prijenose između dvaju nadzornika na odabir nadzorniku.[232] Za prijenose na relaciji nadzornik – obrađivač postoji samo jedna skupina standardnih ugovornih klauzula.[233]

U kontekstu **prava Vijeća Europe**, Savjetodavni odbor Konvencije br. 108 sastavio je vodič za pripremu ugovornih klauzula.[234]

6.4.2. Obvezujuća pravila poduzeća

Višestrana obvezujuća pravila poduzeća (BCR-ovi) vrlo često istovremeno uključuju nekoliko europskih tijela za zaštitu podataka.[235] Kako bi se BCR-ovi odobrili, glavnom tijelu treba poslati prijedlog BCR-ova sa standardiziranim prijavnim obrascima. [236] Glavno tijelo vidljivo je u standardiziranom prijavnom obrascu. Tijelo tada

232 Skupina I. nalazi se u Prilogu Odluke Komisije 2001/497/EZ od 15. lipnja 2001. (Europska komisija (2001)) o standardnim ugovornim klauzulama za prijenos osobnih podataka trećim zemljama prema Direktivi 95/46/EZ, SL 2001 L 181; Skupina II. nalazi se u Prilogu Odluke Komisije 2004/915/EZ od 27. prosinca 2004. (Europska komisija (2004)) o izmjeni Odluke 2001/497/EZ u pogledu uvođenja alternativne skupine standardnih ugovornih klauzula za prijenos osobnih podataka trećim zemljama, SL 2004 L 385.

233 Europska komisija (2010), Odluka Komisije 2010/87 od 5. veljače 2010. o standardnim ugovornim klauzulama za prijenos osobnih podataka izvođačima obrade s poslovnim nastanom u trećim zemljama na temelju Direktive 95/46/EZ Europskog parlamenta i Vijeća, SL 2010 L 39.

234 Vijeće Europe, Savjetodavni odbor Konvencije br. 108 (2002), *Vodič za pripremu ugovornih klauzula kojima se uređuje zaštita podataka tijekom prijenosa osobnih podataka trećim strankama koje nisu obvezane odgovarajućom razinom zaštite podataka.*

235 Sadržaj i struktura odgovarajućih obvezujućih pravila poduzeća objašnjeni su u *Radnom dokumentu o izradi okvira za strukturu obvezujućih pravila za poduzeća* Radne skupine iz članka 29. (2008), WP 154, Bruxelles, 24. lipnja 2008.; i u *Radni dokument o izradi tablice s elementima i načelima iz obvezujućih pravila za poduzeća* Radne skupine iz članka 29. (2008), WP 153, Bruxelles, 24. lipnja 2008.

236 Radna skupina iz članka 29. (2007.), *Preporuka 1/2007 o standardnom zahtjevu za odobrenjem obvezujućih pravila za poduzeća za prijenos osobnih podataka*, WP 133, Bruxelles, 10. siječnja 2007.

obavješćuje sva nadzorna tijela u državama članicama EGP-a u kojima grupacija ima svoje podružnice iako je njihovo sudjelovanje u procesu evaluacije BCR-ova dobrovoljno. Premda to nije obvezujuće, sva predmetna tijela za zaštitu podataka trebala bi ugraditi rezultat evaluacije u svoje službene postupke licenciranja.

6.4.3. Posebni međunarodni sporazumi

Europska unija sklopila je posebne sporazume za dvije vrste prijenosa podataka:

Evidencija imena putnika

Zračne kompanije u postupku rezervacije prikupljaju podatke iz evidencije imena putnika (PNR) koji uključuju imena, adrese, podatke o kreditnoj kartici te brojeve sjedala putnika u zračnom prometu. Prema zakonima SAD-a, zračne kompanije dužne su te podatke staviti na raspolaganje Ministarstvu domovinske sigurnosti prije polaska putnika. To se odnosi na letove u Sjedinjene Američke Države ili iz njih.

Radi osiguranja adekvatne razine zaštite za PNR podatke, a sukladno odredbama Direktive 95/46/EZ, usvojen je "PNR paket"[237] u 2004. godini, koji je osiguravao adekvatnu razinu zaštite za podatke koje bi obrađivao Ministarstvo domovinske sigurnosti SAD-a.

Nastavno na proglašenje PNR paketa nevaljanim od strane CJEU,[238] potpisana su dva zasebna sporazuma s ciljem, u prvom redu, osiguravanja pravne osnove za otkrivanje podataka iz PNR-a stranim tijelima; te u drugom redu uspostavljanja odgovarajuće zaštite podataka u zemlji primateljici.

Prvi sporazum između zemalja Europske unije i Sjedinjenih Američkih Država, o načinu na koji se podaci razmjenjuju i kako se njima upravlja, je potpisan 2007., ali je imao nekoliko nedostataka i zamijenjen je 2012. godine, novim sporazumom koji

237 Odluka Vijeća 2004/496/EZ od 17. svibnja 2004., o potpisivanju Sporazuma između Europske Unije i Sjedinjenih Američkih Država o obradi i prijenosu podataka iz evidencije podataka o putnicima (PNR) zračnih prijevoznika Ministarstvu za domovinsku sigurnost Sjedinjenih Američkih Država, Uredu za carinsku i graničnu zaštitu, SL 2004 L183, str. 83, i Odluka Komisije 2004/535/EZ od 14. svibnja 2004. o adekvatnoj razini zaštite osobnih podataka sadržanih u Evidenciji imena putnika, putnika u zračnom prijevozu, dostavljenih Uredu za carinsku i graničnu zaštitu SAD-a, SL 2004 L 235, str. 11- 22.

238 CJEU, zajednički predmeti C-317/04 i 318/04, Europski parlament protiv Vijeća Europske unije, 30. svibnja 2006, odlomci 57., 58. i 59., kojima je Sud odlučio da su odluka o adekvatnosti zaštite i sporazum o obradi podataka izvan opsega Direktive.

jamči veću pravnu sigurnost.[239] Njime se ograničuju i pojašnjavaju svrhe u koje se informacije mogu koristiti, kao što su ozbiljni transnacionalni zločin i terorizam, te uspostavlja vremensko razdoblje zadržavanja podataka: nakon proteka šest mjeseci podaci se moraju maskirati i depersonalizirati. U slučaju zlouporabe njihovih podataka, svatko ima pravo podnijeti žalbu u upravnom i sudskom postupku u skladu sa zakonodavstvom SAD-a. Također imaju pravo na pristup vlastitim podacima iz PNR-a i, ako su netočni, zatražiti njihov ispravak od Ministarstva domovinske sigurnosti, uključujući mogućnost brisanja.

Sporazum koji je stupio na snagu 1. srpnja 2012. ostaje na snazi sedam godina, do 2019.

U prosincu 2011. Vijeće Europske unije odobrilo je sklapanje ažuriranog Sporazuma između Europske unije i Australije o obradi i prijenosu podataka iz PNR-a.[240] Sporazum između Europske unije i Australije o podacima PNR-a daljnji je korak na dnevnom redu Europske unije koji uključuje globalne smjernice za PNR,[241] izradu sheme EU-PNR [242] i sklapanje sporazuma s trećim zemljama.[243]

Podaci o financijskim porukama

Društvo za svjetsku međubankovnu financijsku telekomunikaciju (SWIFT), sa sjedištem u Belgiji, obrađuje većinu globalnih prijenosa novaca iz europskih banaka. Ono djeluje sa „zrcalnim" računalnim središtem koji nalazi u Sjedinjenim Američkim

239 Odluka Vijeća 2012/472/EU od 26. travnja 2012. o sklapanju Sporazuma između Sjedinjenih Američkih Država i Europske unije o uporabi i prijenosu evidencije imena putnika Ministarstvu domovinske sigurnosti SAD-a, SL 2012 L 215/4. Tekst Sporazuma priložen je ovoj Odluci, SL 2012 L 215, st. 5. - 14.

240 Odluka Vijeća 2012/381/EU od 13. prosinca 2011. o sklapanju Sporazuma između Europske unije i Australije o obradi i prijenosu podataka iz evidencije imena putnika (PNR) od strane zračnih kompanija australskoj Službi za carinsku i graničnu zaštitu, SL 2012 L 186/3. Tekst Sporazuma, kojim se zamjenjuje prethodni sporazum iz 2008., priložen je ovoj Odluci, SL 2012 L 186, str. 4. - 16.

241 Vidjeti naročito Priopćenje Komisije od 21. rujna 2010. o globalnom pristupu prijenosima podataka iz evidencije imena putnika (PNR) trećim zemljama, COM(2010) 492 završno, Bruxelles, 21. rujna 2010. Vidjeti također Mišljenje Radne skupine iz članka 29., *Mišljenje 27/2010 o Komunikaciji Komisije o globalnom pristupu pri iznošenju podataka iz Evidencije imena putnika (PNR) u treće zemlje,* WP 178, Bruxelles, 12. studenog 2010.

242 Prijedlog Direktive Europskog parlamenta i Vijeća o uporabi podataka iz PNR-a za sprečavanje, otkrivanje, istragu i progon terorističkih kaznenih djela i ozbiljnog zločina, COM(2011) 32 završno, Bruxelles, 2. veljače 2011. U travnju 2011. Europski parlament od Europske agencije za temeljna prava zatražio je mišljenje o tom Prijedlogu i njegovoj sukladnosti s Poveljom o temeljnim pravima Europske unije. Vidjeti: FRA (2011), *Mišljenje 1/2011 – Evidencija imena putnika*, Beč, 14. lipnja 2011.

243 Europska unija trenutno dogovara novi sporazum o PNR-u s Kanadom, kojim će se zamijeniti trenutno važeći sporazum iz 2006.

Državama, pa je od SWIFT-a zatraženo da otkrije podatke Ministarstvu financija SAD-a u svrhu istrage terorizma.[244]

S gledišta Europske unije, ne postoji primjerena pravna osnova za otkrivanje tih, u osnovi europskih, podataka kojima se u SAD-u moglo pristupiti samo jer je tamo bio smješten jedan od SWIFT-ovih centara za obradu podataka.

Poseban sporazum između Europske unije i SAD-a, poznat kao Sporazum o SWIFT-u sklopljen je 2010. godine kako bi se osigurala potrebna pravna osnova i odgovarajuća zaštita podataka.[245]

Prema tom sporazumu, financijski podaci koje pohranjuje SWIFT i dalje se dostavljaju Ministarstvu financija SAD-a u svrhu sprečavanja, istrage, otkrivanja ili progona terorizma ili financiranja terorističkih aktivnosti. Ministarstvo financija SAD-a može od SWIFT-a zatražiti financijske podatke pod uvjetom da:

- su financijski podaci u zahtjevu što je jasnije moguće identificirani
- je u zahtjevu jasno potkrijepljena nužnost podataka
- je zahtjev što precizniji kako bi se smanjila količina zatraženih podataka
- se u zahtjevu ne traže podaci koji se odnose na Jedinstveno područje za plaćanje eurom (SEPA).

Europol mora primiti primjerak svakog zahtjeva Ministarstva financija SAD-a i potvrditi poštuju li se načela Sporazuma o SWIFT-u.[246] Ako se potvrdi da se poštuju, SWIFT

244 Vidjeti, u tom kontekstu, Radnu skupinu iz članka 29. (2011), *Mišljenje 14/2011 o pitanjima zaštite podataka vezano uz sprečavanje pranja novca i financiranja terorizma*, WP 186, Bruxelles, 13. lipnja 2011.; Radna skupina iz članka 29. (2006), *Mišljenje 10/2006 o obradi osobnih podataka koju provodi Društvo za svjetsku međubankovnu financijsku telekomunikaciju (SWIFT)*, WP (128), Bruxelles, 22. studenoga 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. prosinca 2008.

245 Odluka Vijeća 2010/412/EU od 13. srpnja 2010. o sklapanju Sporazuma između Europske unije i Sjedinjenih Američkih Država o obradi i prijenosu podataka o financijskih porukama iz Europske unije Sjedinjenim Američkim Državama za potrebe programa praćenja financiranja terorističkih aktivnosti, SL 2010 L 195, str. 3. i 4. Tekst Sporazuma priložen je ovoj Odluci, SL 2010 L 195, str. 5. - 14.

246 Zajedničko nadzorno tijelo Europola je izvršio nadzore nad aktivnostima Europola u ovom području, rezultati nadzora su dostupni na: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

mora financijske podatke dostaviti izravno Ministarstvu financija SAD-a. Ministarstvo mora pohraniti financijske podatke u sigurnom fizičkom okruženju tako da im mogu pristupiti samo analitičari koji istražuju terorizam ili njegovo financiranje, a financijski podaci ne smiju biti međusobno povezani ni sa kojom drugom bazom podataka. Općenito, financijski podaci primljeni od SWIFT-a moraju se izbrisati najkasnije pet godina od primitka. Financijski podaci koji su bitni za određene istrage ili progone mogu se zadržati koliko god dugo su potrebni za te istrage ili progone.

Ministarstvo financija SAD-a može prenijeti informacije iz podataka primljenih od SWIFT-a određenim tijelima policije, javne sigurnosti ili suzbijanja terorizma, unutar ili izvan Sjedinjenih Američkih Država, isključivo radi istrage, otkrivanja, sprečavanja ili progona terorizma i njegova financiranja. Ako daljnji prijenos financijskih podataka uključuje građanina ili državljanina države članice Europske unije, svaka razmjena podataka s tijelima treće zemlje podliježe prethodnoj suglasnosti nadležnih tijela predmetne države članice. Mogu se napraviti izuzeća ako je razmjena podataka nužna za sprečavanje izravne i ozbiljne prijetnje javnoj sigurnosti.

Neovisna tijela koja provode nadzor, uključujući osobu koju imenuje Europska komisija, nadziru sukladnost s načelima Sporazuma o SWIFT-u.

Osobe čiji se podaci obrađuju imaju pravo dobiti potvrdu nadležnog tijela Europske unije za zaštitu podataka o poštivanju svojih prava na zaštitu podataka. Osobe čiji se podaci obrađuju također imaju pravo na ispravak, brisanje ili blokiranje svojih podataka koje prikuplja i pohranjuje Ministarstvo financija SAD-a prema Sporazumu o SWIFT-u. Međutim, prava osoba čiji se podaci obrađuju na pristup mogu podlijegati određenim pravnim ograničenjima. Ako joj je pristup odbijen, osobu čiji se podaci obrađuju treba pisanim putem obavijestiti o odbijanju i o njezinom pravu na žalbu u upravnom i sudskom postupku u Sjedinjenim Američkim Državama.

Sporazum o SWIFT-u vrijedi pet godina, do kolovoza 2015. Automatski se produžuje na daljnja razdoblja od jedne godine osim ako jedna od stranaka obavijesti drugu najmanje šest mjeseci unaprijed o svojoj namjeri da ne produlji sporazum.

7

Zaštita podataka u kontekstu policije i kaznenog pravosuđa

EU	Pitanja kojima se bavi	Vijeće Europe
	Općenito	Konvencija br. 108
	Policija	Preporuka policije
		ECtHR, B.B. protiv Francuske, br. 5335/06, 17. prosinca 2009.
		ECtHR, *S. i Marper protiv Ujedinjene Kraljevine*, br. 30562/04 i 30566/04, 4. prosinca 2008.
		ECtHR, Vetter protiv Francuske, br. 59842/00, 31. svibnja 2005.
	Kibernetički kriminal	Konvencija o kibernetičkom kriminalu
Zaštita podataka u kontekstu prekogranične suradnje policijskih i pravosudnih tijela		
Okvirna odluka o zaštiti podataka	Općenito	Konvencija br. 108
		Preporuka policije
Prümska odluka	Za posebne podatke: otiske prstiju, DNK, huliganizam, itd.	Konvencija br. 108
		Preporuka policije
Odluka Europola	Posebne agencije	Konvencija br. 108
Odluka Eurojusta		Preporuka policije o podacima
Uredba o Frontrexu		
Schengenska odluka II.	Posebni zajednički informacijski sustavi	Konvencija br. 108
Uredba o VIS-u		Preporuka policije
Uredba o Eurodacu		ECtHR, *Dalea protiv Francuske*, br. 964/07, 2. veljače 2010.
Odluka o CIS-u		

Radi uravnoteženja interesa pojedinca za zaštitu podataka i interesa društva za prikupljanje podataka radi suzbijanja zločina i osiguravanja nacionalne i javne sigurnosti, Vijeće Europe i Europska unija usvojile su posebne pravne instrumente.

7.1. Pravo Vijeća Europe o zaštiti podataka u policijskim i kaznenopravnim predmetima

Ključne točke

- Konvencija br. 108 i Preporuka Vijeća Europe o policiji odnose se na zaštitu podataka u svim područjima policijskog rada.
- Konvencija o kibernetičkom kriminalu (*Budimpeštanska konvencija*) obvezujući je međunarodni pravni instrument koji se bavi zločinima počinjenim protiv i putem elektroničkih mreža.

Na europskoj razini, Konvencijom br. 108 obuhvaćena su sva područja obrade osobnih podataka, a svrha je njezinih odredbi općenito urediti obradu osobnih podataka. Stoga se Konvencija br. 108 odnosi na zaštitu podataka u policijskom i kaznenopravnom području, no ugovorne stranke mogu ograničiti njezinu primjenu.

Pravne zadaće policijskih i kaznenopravnih tijela često zahtijevaju obradu osobnih podataka koja može imati ozbiljne posljedice za dotične pojedince. Preporuka o policijskim podacima koju je Vijeće Europe usvojilo 1987. ugovornim strankama pruža smjernice o načinu provedbe načela Konvencije br. 108 u kontekstu obrade osobnih podataka koju provode policijska tijela.[247]

7.1.1. Preporuka o policiji

Stav je Europskog suda za ljudska prava da pohrana i zadržavanje osobnih podataka od strane policijskih ili tijela nacionalne sigurnosti predstavlja zadiranje u članak 8.

247 CoE, Odbor ministara (1987), Preporuka Rec(87)15 državama članicama o korištenju osobnih podataka u policijskom sektoru, 17. rujna 1987.

stavak 1. Europske konvencije o ljudskim pravima. Mnoge se presude Europskog suda za ljudska prava odnose na obrazloženje takvih zadiranja.[248]

Primjer: U predmetu *B.B. protiv Francuske*,[249] Europski sud za ljudska prava odlučio je da uvrštavanje osuđenog seksualnog prijestupnika u nacionalnu pravosudnu evidenciju potpada pod članak 8. Europske konvencije o ljudskim pravima. Međutim, budući da su uvedene odgovarajuće zaštitne mjere, kao što je pravo osobe čiji se podaci obrađuju da zatraži brisanje podataka, ograničeno trajanje pohrane podataka i ograničeni pristup takvim podacima, postignuta je dobra ravnoteža između predmetnih sukobljenih privatnih i javnih interesa. Sud je zaključio da nije prekršen članak 8. Konvencije.

Primjer: U predmetu *S. i Marper protiv Ujedinjene Kraljevine*,[250] oba su podnositelja optužena, ali ne i osuđena, za kaznena djela. No, policija je ipak zadržala i pohranila njihove otiske, DNK profile i stanične uzorke. Neograničeno zadržavanje biometrijskih podataka zakonom je dozvoljeno ako je osoba osumnjičena za kazneno djelo, čak i ako je osumnjičenik kasnije oslobođen od optužbi ili pušten na slobodu. Europski sud za ljudska prava smatrao je da je sveobuhvatno i neselektivno zadržavanje osobnih podataka koje nije vremenski ograničeno i pri kojemu oslobođeni pojedinci imaju samo ograničene mogućnosti zatražiti brisanje predstavljalo nerazmjerno miješanje u prava podnositelja na poštovanje privatnog života. Sud je zaključio da je prekršen članak 8. Konvencije.

Mnoge druge presude Europskog suda za ljudska prava odnose se na obrazloženje miješanja u pravo na zaštitu podataka nadzorom.

Primjer: U predmetu *Allan protiv Ujedinjene Kraljevine*,[251] nadležna su tijela tajno snimala privatne razgovore zatvorenika s prijateljem u zatvorskom prostoru za posjete i sa suoptuženikom u zatvorskoj ćeliji. Europski sud za ljudska prava smatrao je da je uporaba uređaja za audio i video snimanje u podnositeljevoj ćeliji, zatvorskom prostoru za posjete i na kolegi zatvoreniku predstavljala mije-

248 Vidjeti, na primjer, ECtHR, *Leander protiv Švedske*, br. 9248/81, 26. ožujka 1987.; ECtHR, *M.M. protiv Ujedinjene Kraljevine*, br. 24029/07, 13. studenoga 2012; ECtHR, *M.K. protiv Francuske*, br. 19522/09, 18. travnja 2013.

249 ECtHR, *B.B. protiv Francuske*, br. 5335/06, 17. prosinca 2009.

250 ECtHR, *S. i Marper protiv Ujedinjene Kraljevine*, br. 30562/04 i 30566/04, 4. prosinca 2008., st. 119. i 125.

251 ECtHR, *Allan protiv Ujedinjene Kraljevine*, br. 48539/99, 5. studenoga 2002.

šanje u podnositeljevo pravo na privatan život. Budući da nije postojao pravni sustav kojime bi se regulirala policijska uporaba tajnih uređaja za snimanje u danom trenutku, navedeno miješanje nije bilo u skladu sa zakonom. Sud je zaključio da je prekršen članak 8. Konvencije.

Primjer: U predmetu *Klass i drugi protiv Njemačke*,[252] podnositelji su tvrdili da je nekoliko njemačkih zakonodavnih akata kojima se dozvoljava nadzor pošte i telekomunikacija kršilo članak 8. Europske konvencije o ljudskim pravima, naročito jer dotična osoba nije bila obaviještena o nadzornim mjerama i nije se mogla obratiti za pomoć sudovima nakon što su takve mjere ukinute. Europski sud za ljudska prava smatrao je da prijetnja nadzorom svakako ometa slobodu komuniciranja među korisnicima poštanskih i telekomunikacijskih usluga. Međutim, zaključio je da su uvedene odgovarajuće zaštitne mjere protiv zlouporabe. Njemačko je zakonodavstvo opravdano smatralo takve mjere nužnima u demokratskom društvu u interesu nacionalne sigurnosti i radi sprečavanja nereda ili zločina. Sud je zaključio da nije prekršen članak 8. Konvencije.

Budući da obrada podataka koju provode policijska tijela može imati značajan utjecaj na dotične osobe, u tom su području osobito potrebna detaljna pravila za zaštitu podataka koja se odnose na vođenje baza podataka. Svrha Preporuke Vijeća Europe o policiji bila je riješiti to pitanje davanjem smjernica o načinu prikupljanja podataka za potrebe policije; o načinu čuvanja podatkovnih datoteka u tom području; o tome kome je dozvoljen pristup tim datotekama, uključujući uvjete za prijenos podataka stranim policijskim tijelima; o načinu na koji osobe čiji se podaci obrađuju trebaju moći ostvariti svoja prava na zaštitu podataka; i o načinu na koji neovisna tijela trebaju provoditi kontrolu. Razmatra se i obveza osiguravanja odgovarajuće razine sigurnosti podataka.

Preporukom se ne propisuje otvoreno, neselektivno prikupljanje podataka policijskih tijela. Ograničuje se prikupljanje osobnih podataka koje provode policijska tijela na mjeru nužnu za sprečavanje stvarne opasnosti ili suzbijanje određenog kaznenog djela. Svako dodatno prikupljanje podataka trebalo bi se temeljiti na posebnom nacionalnom zakonodavstvu. Obrada osjetljivih podataka treba biti ograničena na mjeru koja je apsolutno nužna u kontekstu određenog upita.

Ako se osobni podaci prikupljaju bez znanja osobe čiji se podaci obrađuju, osoba čiji se podaci obrađuju treba biti informirana o prikupljanju podataka čim otkrivanje više

252 ECtHR, *Klass i drugi protiv Njemačke*, br. 5029/71, 6. rujna 1978.

ne ometa istragu. Prikupljanje podataka tehničkim nadzorom ili drugim automatskim sredstvima također se treba temeljiti na posebnim pravnim odredbama.

> Primjer: U predmetu *Vetter protiv Francuske*[253] anonimni su svjedoci podnositelja optužili za ubojstvo. Budući da je podnositelj redovito posjećivao prijateljevu kuću, policija je u njoj postavila uređaje za prisluškivanje uz dozvolu istražnog suca. Podnositelj je uhićen na temelju snimljenih razgovora i suđeno mu je zbog ubojstva. Zatražio je da se snimka proglasi neprihvatljivim dokazom tvrdeći da nije pribavljena na način predviđen zakonom. Europski sud za ljudska prava trebao je odlučiti je li uporaba prislušnih uređaja bila „u skladu sa zakonom." Postavljanje prislušnih uređaja u privatne prostorije nedvojbeno nije unutar opsega primjene članka 100. i nastavnih članaka Zakona o kaznenom postupku jer se te odredbe odnose na prisluškivanje telefonskih linija. U članku 81. Zakona nije dovoljno jasno naveden opseg primjene ili način na koji nadležna tijela po vlastitom nahođenju odlučuju o nadzoru privatnih razgovora. U skladu s time, podnositelj nije imao najmanju razinu zaštite na koju građani imaju pravo u skladu s vladavinom prava u demokratskom društvu. Sud je zaključio da je prekršen članak 8. Konvencije.

U preporuci je naveden zaključak da pri pohrani osobnih podataka treba jasno razlikovati: administrativne podatke od policijskih podataka; vrste osoba čiji se podaci obrađuju, kao što su osumnjičenici, osuđenici, žrtve i svjedoci; i podatke koji se smatraju čvrstim činjenicama od onih koji se temelje na sumnjama ili nagađanjima.

Policijske podatke treba strogo ograničiti s obzirom na svrhu. To utječe na priopćavanje policijskih podataka trećim strankama: prijenos ili priopćavanje takvih podataka unutar policijskog sektora treba ovisiti o tome postoji li legitiman interes za dijeljenjem informacija. Prijenos ili priopćavanje takvih podataka izvan policijskog sektora trebaju biti dozvoljeni samo ako postoji jasna pravna obveza ili ovlaštenje. Međunarodni prijenos ili priopćavanje trebaju biti ograničeni na strana policijska tijela i temeljiti se na posebnim pravnim odredbama, kao što su međunarodni sporazumi, osim ako je to potrebno radi sprečavanja ozbiljne i neposredne opasnosti.

Obrada podataka koju provodi policija mora podlijegati neovisnom nadzoru radi osiguravanja sukladnosti s nacionalnim zakonodavstvom o zaštiti podataka. Osobe čiji se podaci obrađuju moraju imati sva prava na pristup iz Konvencije br. 108. Ako su

253 ECtHR, *Vetter protiv Francuske*, br. 59842/00, 31. svibnja 2005.

prava osoba čiji se podaci obrađuju na pristup ograničena prema članku 9. Konvencije br. 108 u interesu učinkovitih policijskih istraga, osoba čiji se podaci obrađuju mora imati pravo prema nacionalnom zakonodavstvu na žalbu nacionalnom nadzornom tijelu za zaštitu podataka ili drugom neovisnom tijelu.

7.1.2. Budimpeštanska konvencija o kibernetičkom kriminalu

Budući da se u kriminalnim aktivnostima sve češće koriste elektronički sustavi za obradu podataka, a kriminalne aktivnosti utječu na te sustave, potrebne su nove kaznenopravne odredbe kojima se rješava taj problem. Stoga je Vijeće Europe usvojilo međunarodni pravni instrument, Konvenciju o kibernetičkom kriminalu – poznatu i kao Budimpeštanska konvencija – kako bi riješila problem zločina počinjenih protiv i putem elektroničkih mreža.[254] Toj konvenciji mogu pristupiti i države koje nisu članice Vijeća Europe. Do sredine 2013., četiri države izvan Vijeća Europe – Australija, Dominikanska Republika, Japan i Sjedinjene Američke Države – bile su stranke konvencije, a 12 drugih država koje nisu članice Vijeća Europe potpisale su je ili su pozvane da joj pristupe.

Konvencija o kibernetičkom kriminalu i dalje je najutjecajniji međunarodni sporazum koji se bavi kršenjima prava putem internetskih ili drugih informacijskih mreža. Njezine stranke moraju ažurirati i uskladiti svoje kaznene zakone protiv hakiranja i ostalih povreda sigurnosti uključujući povrede autorskih prava, računalno potpomognutu prijevaru, dječju pornografiju i druge zabranjene kibernetičke aktivnosti. Konvencijom su propisane i proceduralne ovlasti koje obuhvaćaju pretraživanje računalnih mreža i presretanje komunikacija u kontekstu suzbijanja kibernetičkog kriminala. Naposljetku, njome je omogućena učinkovita međunarodna suradnja. Dodatni protokol uz konvenciju bavi se inkriminacijom rasističke i ksenofobne propagande u računalnim mrežama.

Iako konvencija zapravo nije instrument za promicanje zaštite podataka, njome se inkriminiraju aktivnosti za koje je izgledno da će prekršiti prava osobe čiji se podaci obrađuju na zaštitu njezinih podataka. Njome se ugovorne stranke također obvezuju da pri provedbi konvencije predvide odgovarajuću zaštitu ljudskih prava i sloboda,

254 Vijeće Europe, Odbor Ministara (2001), Konvencija o kibernetičkom kriminalu, CETS br. 185, Budimpešta, 23. studenoga 2001., stupila na snagu 1. srpnja 2004.

uključujući prava zajamčena Europskom konvencijom o ljudskim pravima, kao što je pravo na zaštitu podataka.[255]

7.2. Pravo Vijeća Europe o zaštiti podataka u policijskim i kaznenopravnim predmetima

Ključne točke

- Na razini Europske unije, zaštita podataka u policijskom i kaznenopravnom sektoru uređena je samo u kontekstu prekogranične suradnje policije i pravosudnih tijela.
- Za Europski policijski ured (Europol) i Jedinicu Europske unije za pravosudnu suradnju (Eurojust), tijela Europske unije koja pomažu i promiču prekograničnu provedbu zakona, postoje posebni režimi zaštite podataka.
- Posebni režimi zaštite podataka postoje i za zajedničke informacijske sustave uspostavljene na razini Europske unije za prekograničnu razmjenu informacija između nadležnih policijskih i pravosudnih tijela. Važni su primjeri Schengen II, vizni informacijski sustav (VIS) i Eurodac, centralizirani sustav s podacima o otiscima prstiju stanovnika trećih zemalja koji su podnijeli zahtjev za azil u jednoj od država članica Europske unije.

Direktiva o zaštiti podataka ne odnosi se na područje policije i kaznenog pravosuđa. U odjeljak 7.2.1 opisani su najvažniji pravni instrumenti u tom području.

7.2.1. Okvirna odluka o zaštiti podataka

Cilj je Okvirne odluke Vijeća 2008/977/PUP o zaštiti osobnih podataka koji se obrađuju u okviru suradnje policije i pravosudnih tijela u kaznenopravnim predmetima (*Okvirna odluka o direktivi o zaštiti podataka*)[256] osigurati zaštitu osobnih podataka fizičkih osoba kad se njihovi podaci obrađuju u svrhu sprečavanja, istrage, otkrivanja ili progona kaznenog djela ili izvršavanja kazni. U ime država članica ili Europske unije djeluju nadležna tijela koja rade u području policije i kaznenog pravosuđa. Ta su tijela agencije ili tijela Europske unije, kao i tijela država članica.[257] Primjenjivost

255 *Ibid.,* čl.15. st. 1.

256 Vijeće Europske unije (2008), Okvirna odluka Vijeća 2008/977/PUP od 27. studenoga 2008. o zaštiti osobnih podataka koji se obrađuju u okviru suradnje policije i kaznenog pravosuđa u kaznenopravnim predmetima (*Okvirna odluka o zaštiti podataka*), SL 2008 L 350.

257 *Ibid.,* čl. 2. točka (h).

okvirne odluke ograničena je na osiguravanje zaštite podataka u prekograničnoj suradnji među tim tijelima i ne proteže se na nacionalnu sigurnost.

Okvirna odluka o zaštiti podataka u velikoj se mjeri oslanja na načela i definicije sadržane u Konvenciji br. 108 i Direktivi o zaštiti podataka.

Podatke smije koristiti samo nadležno tijelo i samo u svrhu u koju su preneseni ili stavljeni na raspolaganje. Država članica primateljica mora poštivati sva ograničenja o razmjeni podataka koja su propisana zakonodavstvom države članice koja prenosi podatke. Međutim, država koja prima podatke smije koristiti podatke u druge svrhe pod određenim uvjetima. Bilježenje i dokumentiranje prijenosa posebne su dužnosti nadležnih tijela radi pomaganja u pojašnjenju odgovornosti koje proizlaze iz pritužbi. Za daljnji prijenos podataka primljenih tijekom prekogranične suradnje trećim strankama potrebna je suglasnost države članice iz koje potječu podaci, no postoje i izuzeća u hitnim slučajevima.

Nadležna tijela moraju poduzeti potrebne mjere sigurnosti kako bi zaštitila osobne podatke od nezakonitog oblika obrade.

Svaka država članica mora osigurati da je jedno ili više neovisnih nacionalnih nadzornih tijela odgovorno za savjetovanje i nadzor primjene odredbi usvojenih u skladu s Okvirnom odlukom o zaštiti podataka. Moraju također saslušati zahtjeve koje podnese bilo koja osoba u vezi sa zaštitom njezinih prava i sloboda u pogledu obrade osobnih podataka od strane nadležnih tijela.

Osoba čiji se podaci obrađuju ima pravo na informacije o obradi svojih podataka i ima pravo na pristup, ispravak, brisanje ili blokiranje. Ako je ostvarenje tih prava odbijeno na uvjerljivoj osnovi, osoba čiji se podaci obrađuju mora imati pravo na žalbu nadležnom nacionalnom nadzornom tijelu i/ili sudu. Ako osoba pretrpi štetu zbog kršenja nacionalnog zakonodavstva kojime se provodi Okvirna odluka o zaštiti podataka, ima pravo na naknadu od nadzornika.[258] Općenito, osobe čiji se podaci obrađuju moraju imati na raspolaganju pravni lijek u slučaju kršenja prava koja su im zajamčena nacionalnim zakonodavstvom kojime se provodi Okvirna odluka o zaštiti podataka.[259]

258 *Ibid.,* čl. 19.

259 *Ibid.,* čl. 20.

Europska komisija predložila je reformu koja se sastoji od Opće uredbe o zaštiti podataka,[260] i Opće direktive o zaštiti podataka.[261] Tom se novom direktivom zamjenjuje trenutna Okvirna odluka o zaštiti podataka i primjenjuju opća načela i pravila na suradnju policije i pravosudnih tijela u kaznenopravnim predmetima.

7.2.2. Specifičniji pravni instrumenti za zaštitu podataka u prekograničnoj suradnji policije i tijela za provedbu zakona

Osim Okvirnom odlukom o zaštiti podataka, razmjena informacija u posjedu država članica u posebnim područjima regulirana je nizom pravnih instrumenata kao što su Okvirna odluka Vijeća 2009/315/PUP o organizaciji i sadržaju razmjene podataka iz kaznene evidencije između država članica i Odluka Vijeća o uređenju suradnje između financijsko-obavještajnih jedinica država članica u vezi s razmjenom podataka.[262]

Bitno je napomenuti da prekogranična suradnja[263] nadležnih tijela sve više uključuje razmjenu imigracijskih podataka. To područje prava nije u nadležnosti policijskih i kaznenopravnih predmeta, no u mnogočemu je relevantno za rad policije i pravosudnih tijela. Isto vrijedi za podatke o robi koja se uvozi u Europsku uniju ili izvozi iz nje. Ukidanje unutarnjih graničnih kontrola u Europskoj uniji povećalo je rizik od prijevare pa države članice moraju pojačati suradnju, naročito poboljšanjem prekogranične razmjene podataka radi učinkovitijeg otkrivanja i progona kršenja nacionalnog prava i carinskog prava Europske unije.

260 Europska komisija (2012.), *Prijedlog Uredbe Europskog parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (Opća uredba o zaštiti podataka)*, COM(2012) 11 konačno, Bruxelles, 25. siječnja 2012.

261 Europska komisija (2012.), *Prijedlog Direktive Europskog parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka u ovlaštenim tijelima u svrhe sprečavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kazni te o slobodnom protoku takvih podataka (Opća direktiva o zaštiti podataka)*, COM(2012) 10 konačno, Bruxelles, 25. siječnja 2012.

262 Vijeće Europske unije (2009), Okvirna odluka Vijeća 2009/315/PUP od 26. veljače 2009. o organizaciji i sadržaju razmjene podataka iz kaznene evidencije između država članica, SL 2009 L 93; Vijeće Europske unije (2009), Odluka Vijeća 2000/642/PUP od 17. listopada 2000. o uređenju suradnje između financijsko-obavještajnih jedinica država članica u vezi s razmjenom podataka, SL 2000 L 271.

263 Europska komisija (2012), Priopćenje Komisije Europskom parlamentu i Vijeću - Jačanje policijske suradnje u Europskoj uniji - Europski model razmjene podataka (EIXM), COM(2012) 735 završno, Bruxelles, 7. prosinca 2012.

Prümska odluka

Važan primjer institucionalizacije prekogranične suradnje razmjenom podataka koji se čuvaju na nacionalnoj razini jest Odluka Vijeća 2008/615/PUP o produbljivanju prekogranične suradnje, posebno u suzbijanju terorizma i prekograničnog kriminala (*Prümska odluka*) kojom je Prümski ugovor ugrađen u pravo Europske unije 2008. godine.[264] Prümski ugovor je ugovor o međunarodnoj policijskoj suradnji koji su 2005. potpisali Austrija, Belgija, Francuska, Njemačka, Luksemburg, Nizozemska i Španjolska.[265]

Cilj je Prümske odluke državama članicama pomoći u poboljšanju razmjene informacija radi sprečavanja i suzbijanja kriminala u trima područjima: terorizmu, prekograničnom kriminalu i nezakonitoj migraciji. U tu se svrhu u odluci navode odredbe u pogledu:

- automatiziranog pristupa DNK profilima, podataka o otiscima prstiju i određenih nacionalnih podataka o registraciji vozila
- dostave podataka u vezi s važnim događajima prekogranične naravi
- dostave informacija radi sprečavanja terorističkih kaznenih djela
- drugih mjera za produbljivanje prekogranične policijske suradnje.

Za baze podataka koje se stavljaju na raspolaganje prema Prümskoj odluci u potpunosti je nadležno nacionalno zakonodavstvo, no razmjena podataka dodatno je uređena odlukom i, odnedavno, Okvirnom odlukom o zaštiti podataka. Tijela nadležna za nadzor takvih prijenosa podataka su nacionalna nadzorna tijela za zaštitu podataka.

264 Vijeće Europske unije (2008), Odluka Vijeća 2008/615/PUP od 23. lipnja 2008. o produbljivanju prekogranične suradnje, posebno u suzbijanju terorizma i prekograničnog kriminala, SL 2008 L 210.

265 Konvencija između Kraljevine Belgije, Savezne Republike Njemačke, Kraljevine Švedske, Republike Francuske, Velikog Vojvodstva Luksemburga, Kraljevine Nizozemske i Republike Austrije o o produbljivanju prekogranične suradnje, posebno u suzbijanju terorizma, prekograničnog kriminala i nezakonite migracije, dostupno na: http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.

7.2.3. Zaštita podataka u Europolu i Eurojustu

Europol

Europol, agencija za provedbu prava Europske unije sa sjedištem u Haagu ima Europolove nacionalne jedinice (ENU-ove) u svakoj državi članici. Europol je osnovan 1998.; njegov trenutačni pravni status institucije Europske unije temelji se na Odluci Vijeća o osnivanju Europskog policijskog ureda (*Odluka o Europolu*).[266] Cilj je Europola pomoći u sprečavanju i istrazi organiziranog kriminala, terorizma i drugih oblika teškog kriminala koji se tiču dviju ili više država članica, kako je navedeno u Prilogu Odluke o Europolu.

Radi ostvarenja svog cilja, Europol je uspostavio Europolov informacijski sustav s bazom podataka temeljem koje države članice razmjenjuju obavijesti i informacije o kriminalu putem svojih ENU-ova. Europolov informacijski sustav može se koristiti radi stavljanja na raspolaganje podataka koji se odnose na: osobe koje su osumnjičene ili osuđene za kazneno djelo u nadležnosti Europola; ili osobe za koje se opravdano sumnja da će takva djela počiniti. Europol i ENU-ovi mogu izravno unijeti podatke u Europolov sustav informacija i preuzeti ih iz njega. Podatke može izmijeniti, ispraviti ili izbrisati samo stranka koja ih je unijela u sustav.

Ako je to nužno za izvršavanje njegovih zadaća, prilikom analize radnih datoteka Europol može pohraniti, izmijeniti i upotrijebiti podatke koji se odnose na kaznena djela. Radne datoteke za analizu otvorene su u svrhu prikupljanja, obrade ili uporabe podataka radi pomaganja u određenim kaznenim istragama koje Europol provodi zajedno s državama članicama Europske unije.

Kako bi se suočio s novim promjenama, 1. siječnja 2013. Europol je osnovao Europski centar za kibernetički kriminal.[267] Centar ima ulogu središta Europske unije za kibernetički kriminal čime se omogućuje brže reagiranje u slučaju internetskih zločina, razvijanje i primjena digitalnih forenzičkih rješenja i provodi najbolja praksa u istragama kibernetičkog kriminala. Centar se bavi kibernetičkim kriminalom koji:

266 Vijeće Europske unije (2009), Odluka Vijeća od 6. travnja 2009. o osnivanju Europskog policijskog ureda, SL L 2009 L 121 (Europol). Vidjeti također prijedlog uredbe Komisije u kojemu se propisuje pravni okvir za novi Europol koji nasljeđuje i zamjenjuje Europol kako je utvrđeno Odlukom Vijeća 2009/371/PUP od 6. travnja 2009. o osnivanju Europskog policijskog ureda (Europol) i CEPOL, kako je utvrđeno Odlukom Vijeća 2005/681/PUP o osnivanju Europske visoke policijske škole (CEPOL), COM(2013) 173 završno.

267 Vidjeti također EDPS (2012), *Mišljenje Nadzornika za zaštitu podataka o priopćenju Europske komisije Vijeću i Europskom parlamentu o osnivanju Europskog centra za kibernetički kriminal,* Bruxelles, 29. lipnja 2012.

- su počinile organizirane skupine radi ostvarivanja velikih kriminalnih dobiti, kao što je internetska prijevara

- uzrokuje veliku štetu žrtvi, na primjer, seksualno iskorištavanje djece putem interneta

- utječe na ključnu infrastrukturu i informacijske sustave u Europskoj uniji.

Poboljšan je režim zaštite podataka koji upravlja aktivnostima Europola. U članku 27. Odluke o Europolu navodi se da vrijede načela navedena u Konvenciji br. 108 i Preporuci o policijskim podacima u vezi s obradom automatiziranih i neautomatiziranih podataka. Prijenos podataka između Europola i država članica također mora biti u skladu s pravilima iz Okvirne odluke o zaštiti podataka.

Neovisno Europolovo Zajedničko nadzorno tijelo pregledava i nadzire aktivnosti Europola kako bi se osigurala sukladnost s primjenjivim zakonodavstvom o zaštiti podataka, točnije, kako se prava pojedinca ne bi kršila obradom osobnih podataka.[268] Svaki pojedinac ima pravo na pristup svim osobnim podacima koje o njemu posjeduje Europol, kao i pravo traženja provjere, ispravka ili brisanja tih osobnih podataka. Ako osoba nije zadovoljna Europolovom odlukom u vezi s ostvarenjem tih prava, može se žaliti Žalbenom odboru Zajedničkog nadzornog tijela.

Ako je do štete došlo zbog pravnih ili činjeničnih pogrešaka u podacima koji se pohranjuju ili obrađuju u Europolu, oštećena strana može se žaliti samo nadležnom sudu države članice u kojoj se odvio događaj koji je prouzročio štetu.[269] Europol mora nadoknaditi štetu državi članici ako je do štete došlo zbog toga što Europol nije ispunio svoje pravne obveze.

268 Odluka o Europolu, čl. 34.

269 *Ibid.,* čl. 52.

Eurojust

Eurojust, tijelo Europske unije osnovano 2002. sa sjedištem u Haagu, promiče pravosudnu suradnju u istragama i progonima teških zločina koji uključuju barem dvije države članice.[270] Eurojust je ovlašten:

- poticati i unapređivati koordinaciju istraga i progona među nadležnim tijelima raznih država članica

- omogućiti izvršavanje zahtjeva i odluka koji se odnose na pravosudnu suradnju.

Funkcije Eurojusta vrše nacionalni članovi. Svaka država članica imenuje po jednog suca ili tužitelja Eurojusta s potrebnim stručnim vještinama za izvršavanje zadaća potrebnih za poticanje i unapređenje pravosudne suradnje. Status tog suca ili tužitelja podliježe nacionalnom zakonodavstvu. Osim toga, nacionalni članovi zajednički su okupljeni u kolegij radi izvršavanja posebnih Eurojustovih zadaća.

Eurojust može obrađivati osobne podatke ako je to potrebno da bi ostvario svoje ciljeve. Ta je mogućnost ipak ograničena na određene informacije u vezi s osobama osumnjičenim za počinjenje kaznenog djela ili sudjelovanje u njemu, ili osuđenim za kazneno djelo u nadležnosti Eurojusta. Eurojust može obrađivati i informacije u vezi sa svjedocima ili žrtvama kaznenih djela iz nadležnosti Eurojusta.[271] U iznimnim okolnostima i tijekom ograničenog vremenskog razdoblja Eurojust može obrađivati širi raspon osobnih podataka u vezi s okolnostima kaznenog djela ako se takvi podaci neposredno odnose na istragu u tijeku. Unutar područja nadležnosti, Eurojust može surađivati s drugim institucijama, tijelima i agencijama Europske unije i s njima razmjenjivati osobne podatke. Eurojust može surađivati i razmjenjivati podatke i s trećim zemljama i organizacijama.

U vezi sa zaštitom podataka, Eurojust mora jamčiti razinu zaštite barem jednaku načelima Konvencije br. 108 Vijeća Europe i njezinim kasnijim izmjenama. Pri razmjeni podataka moraju se poštivati posebna pravila i ograničenja uvedena bilo

270 Vijeće Europske unije (2002), Odluka Vijeća 2002/287/PUP od 28. veljače 2002. o osnivanju Eurojusta s ciljem jačanja borbe protiv teškog kriminala, SL 2002 L 63; Vijeće Europske unije (2003), Odluka Vijeća 2003/659/PUP od 18. lipnja 2003. o izmjeni Odluke 2002/187/PUP o osnivanju Eurojusta s ciljem jačanja borbe protiv teškog kriminala, SL 2003 L 44; Vijeće Europske unije (2009), Odluka Vijeća 2009/426/PUP od 16. prosinca 2008. o jačanju Eurojusta i izmjeni Odluke 2002/187/PUP o osnivanju Eurojusta s ciljem jačanja borbe protiv teškog kriminala, SL 2009 L 138 (*Odluke o Eurojustu*).

271 Pročišćena verzija Odluke Vijeća 2002/187/PUP kako je izmijenjena Odlukom Vijeća 2003/659/PUP i Odlukom Vijeća 2009/426/PUP, čl. 15. st. 2.

sporazumom o suradnji ili radnim dogovorom u skladu s Odlukama Vijeća o Europolu i Pravilima o zaštiti podataka u Eurojustu.[272]

U okviru Eurojusta osnovano je Zajedničko nadzorno tijelo sa zadaćom nadzora obrade osobnih podataka koju provodi Eurojust. Pojedinci se mogu žaliti Zajedničkom nadzornom tijelu ako nisu zadovoljni Eurojustovim odgovorom na zahtjev za pristupom, ispravkom, blokiranjem ili brisanjem osobnih podataka. Ako Eurojust takve osobne podatke obrađuje nezakonito, Eurojust odgovara u skladu s nacionalnim zakonodavstvom države članice u mjestu njegova sjedišta, Nizozemskoj, zbog štete prouzročene osobi čiji se podaci obrađuju.

7.2.4. Zaštita podataka u zajedničkim informacijskim sustavima na razini Europske unije

Osim razmjene podataka među državama članicama i osnivanja specijaliziranih tijela Europske unije za suzbijanje prekograničnog kriminala, na razini Europske unije uspostavljeno je nekoliko zajedničkih informacijskih sustava koji služe kao platforma za razmjenu podataka između nadležnih nacionalnih i tijela Europske unije u posebne svrhe provedbe zakona, uključujući imigracijsko i carinsko pravo. Neki su se od ovih sustava razvili iz višestranih sporazuma koji su kasnije nadopunjeni pravnim instrumentima i sustavima Europske unije, kao što su Schengenski informacijski sustav, vizni informacijski sustav, Eurodac, Eurosur ili carinski informacijski sustav.

Europska agencija za velike informatičke sustave (eu-LISA),[273] osnovana 2012., odgovorna je za dugoročno operativno upravljanje Schengenskim informacijskim sustavom druge generacije (SIS II), viznim informacijskim sustavom (VIS) i Eurodacom. Osnovna zadaća agencije eu-LISA je osigurati učinkovit, siguran i neprekidan rad informatičkih sustava. Odgovorna je i za usvajanje potrebnih mjera sigurnosti sustava i podataka.

Schengenski informacijski sustav

Godine 1985. nekoliko je država članica bivših Europskih zajednica sklopilo Sporazum s državama Gospodarske unije Beneluksa, Njemačkom i Francuskom o

272 Poslovnik o obradi i zaštiti osobnih podataka u Eurojustu, SL 2005 C 68/01, 19. ožujka 2005., str. 1.

273 Uredba (EU) br. 1077/2011 Europskog parlamenta i Vijeća od 25. listopada 2011. o osnivanju Europske agencije za operativno upravljanje velikim informatičkim sustavima u području slobode, sigurnosti i pravde, SL 2011 L 286.

postupnom ukidanju kontrola na zajedničkim granicama (*Schengenski sporazum*) kako bi se stvorio prostor za slobodno kretanje osoba, neometan graničnim kontrolama unutar schengenskog prostora.[274] Kao protuteža prijetnji javnoj sigurnosti uslijed otvaranja granica, uspostavljene su pojačane granične kontrole na vanjskim granicama schengenskog prostora kao i uska suradnja nacionalne policije i pravosudnih tijela.

Budući da je Schengenskom sporazumu pristupilo još država, schengenski je sustav konačno integriran u pravni okvir Europske unije Ugovorom iz Amsterdama.[275] Ta je odluka provedena 1999. Najnovija verzija Schengenskog informacijskog sustava, takozvani SIS II, puštena je u rad 9. travnja 2013. Trenutno se njome služe sve države članice Europske unije kao i Island, Lihtenštajn, Norveška i Švicarska.[276] Europol i Eurojust također imaju pristup sustavu SIS II.

SIS II sastoji se od središnjeg sustava (C-SIS), nacionalnog sustava (N-SIS) u svakoj državi članici i komunikacijske infrastrukture između središnjeg sustava i nacionalnih sustava. C-SIS sadrži određene podatke o osobama i predmetima koje unose države članice. C-SIS koriste nacionalna tijela za graničnu kontrolu, policijska, carinska, vizna i pravosudna tijela diljem schengenskog prostora. Svaka od država članica upravlja nacionalnom kopijom sustava C-SIS, poznatom kao nacionalni Schengenski informacijski sustav (N-SIS) koji se stalno ažurira, čime se ažurira i C-SIS. N-SIS se pregledava i šalje upozorenje ako:

- osoba nema pravo ući ili ostati u schengenskom prostoru
- osobu ili predmet traže pravosudna ili policijska tijela
- je osoba prijavljena kao nestala
- je roba, poput novčanica, automobila, kamiona, vatrenog oružja i identifikacijskih dokumenata, prijavljena kao ukradena ili izgubljena imovina.

274 Sporazum među vladama država Gospodarske unije Beneluksa, Savezne Republike Njemačke i Francuske Republike o postupnom ukidanju kontrola na zajedničkim granicama, SL 2000 L 239.

275 Europske zajednice (1997), Ugovor iz Amsterdama o izmjenama Ugovora o Europskoj uniji, ugovora o osnivanju Europskih zajednica i određenih srodnih akata, SL 1997 C 340.

276 Uredba (EZ) br. 1987/2006 Europskog parlamenta i Vijeća od 20. prosinca 2006. o osnivanju, radu i uporabi druge generacije Schengenskog informacijskog sustava, SL 2006 L 381 (*SIS II*) i Vijeće Europske unije (2007), Odluka Vijeća 2007/533/PUP od 12. lipnja 2007. o osnivanju, radu i uporabi druge generacije Schengenskog informacijskog sustava (*SIS II*), SL 2007 L 205.

U slučaju upozorenja treba pokrenuti prateće aktivnosti putem nacionalnih Schengenskih informacijskih sustava.

SIS II ima nove funkcionalnosti kao što je mogućnost unosa: biometrijskih podataka, poput otisaka prstiju i fotografija; ili novih vrsta upozorenja, poput ukradenih plovila, zrakoplova, spremnika ili sredstava plaćanja; i pojačanih upozorenja o osobama i objektima; kopija europskih uhidbenih naloga (EAW-ova) o osobama traženima radi uhićenja, predaje ili izručenja.

U Odluku Vijeća 2007/533/PUP o osnivanju, radu i uporabi druge generacije Schengenskog informacijskog sustava (Schengenska odluka II.) ugrađena je Konvencija br. 108. „Osobni podaci koji se obrađuju primjenjujući ovu odluku zaštićeni su u skladu s Konvencijom br. 108 Vijeća Europe."[277] Ako nacionalna policijska tijela koriste osobne podatke primjenjujući Schengensku odluku II., odredbe Konvencije br. 108 kao i Preporuke o policijskim podacima moraju se uvesti u nacionalno zakonodavstvo.

Nadležno nacionalno nadzorno tijelo u svakoj državi članici nadzire nacionalni N-SIS. Točnije, ono provjerava kvalitetu podataka koje država članica unosi u sustav SIS putem sustava N-SIS, a Europski nadzornik za zaštitu osobnih podataka je nadležan za nadzor sustava C-SIS. Nacionalno nadzorno tijelo osigurava reviziju postupaka obrade podataka unutar nacionalnog sustava N-SIS barem svake četiri godine. Nacionalna nadzorna tijela i Europski nadzornik za zaštitu podataka surađuju i osiguravaju usklađeni nadzor sustava C-SIS. Radi transparentnosti, Europskom parlamentu, Vijeću i agenciji eu-LISA šalje se zajedničko izvješće o aktivnostima.

Prava pojedinaca na pristup koja se odnose na SIS II mogu se ostvariti u bilo kojoj državi članici jer je svaki N-SIS precizna kopija sustava C-SIS.

Primjer: U predmetu *Dalea protiv Francuske*,[278] podnositelju je odbijen zahtjev za vizom radi posjeta Francuskoj jer su francuske vlasti Schengenskom informacijskom sustavu javile da mu se ne smije odobriti ulaz. Podnositelj je neuspješno tražio pristup i ispravljanje ili brisanje podataka pred francuskom Komisijom za zaštitu podataka i, konačno, pred Državnim vijećem. Europski sud za ljudska prava smatrao je da je prijava podnositelja Schengenskom informacijskom

277 Vijeće Europske unije (2007), Odluka Vijeća 2007/533/PUP od 12. lipnja 2007. o osnivanju, radu i uporabi druge generacije Schengenskog informacijskog sustava, SL 2007 L 205, čl. 57.

278 ECtHR, *Dalea protiv Francuske* (dec.), br. 964/07, 2. veljače 2010.

sustavu bila u skladu sa zakonom i legitimnom svrhom zaštite nacionalne sigurnosti. Budući da podnositelj nije pokazao kako je zapravo bio oštećen uskratom ulaska u schengenski prostor i budući da su se primjenjivale odgovarajuće mjere kojima je bio zaštićen od proizvoljnih odluka, miješanje u njegovo pravo na poštovanje privatnog života bilo je razmjerno. Stoga je podnositeljeva pritužba na temelju članka 8. proglašena neprihvatljivom.

Vizni informacijski sustav

Vizni informacijski sustav (VIS), kojim također upravlja eu-LISA, razvijen je kao podrška provedbi zajedničke vizne politike Europske unije.[279] Zahvaljujući sustavu VIS, schengenske države mogu razmjenjivati vizne podatke putem sustava koji povezuje konzulate schengenskih država u državama izvan Europske unije s vanjskim pograničnim točkama svih schengenskih država. U VIS-u se obrađuju podaci u vezi sa zahtjevima za vizama za kratkotrajni boravak ili za provozom kroz schengenski prostor. Uz pomoć biometrijskih podataka, sustav VIS pograničnim tijelima omogućuje provjeru je li osoba koja je predočila vizu njen valjani imatelj kao i identifikaciju osoba bez ikakvih dokumenata ili s lažnim dokumentima.

Prema Uredbi (EZ) br. 767/2008 Europskog parlamenta i Vijeća o viznom informacijskom sustavu (VIS) i razmjeni podataka među državama članicama o vizama za kratkotrajni boravak (*Uredba o VIS-u*), u VIS-u se smiju bilježiti samo podaci o podnositelju, njegove vize, fotografije, otisci prstiju, poveznice s prethodnim prijavama i prijavne datoteke osoba u pratnji podnositelja.[280] Pristup VIS-u radi unosa, izmjene ili brisanja podataka ograničen je isključivo na tijela država članica nadležna za izdavanje viza, dok je pristup radi uvida u podatke osiguran tijelima nadležnim za izdavanje viza i onima nadležnim za kontrole na vanjskim pograničnim točkama, imigracijske kontrole i azil. U određenim okolnostima nacionalna nadležna policijska tijela

279 Vijeće Europske unije (2004), Odluka Vijeća od 8. lipnja 2004.o osnivanju viznog informacijskog sustava (VIS), SL 2004 L 213; Uredba (EZ) br. 767/2008 Europskog parlamenta i Vijeća od 9. srpnja 2008. o viznom informacijskom sustavu (VIS) i razmjeni podataka među državama članicama o vizama za kratkotrajni boravak, SL 2008 L 218 (*Uredba o VIS-u*); Vijeće Europske unije (2008), Odluka Vijeća 2008/633/PUP od 23. lipnja 2008. o pristupu određenih tijela država članica i Europola viznom informacijskom sustavu (VIS) za traženje podataka u svrhu sprečavanja, otkrivanja i istraga terorističkih kaznenih djela i ostalih teških kaznenih djela, SL 2008 L 218.

280 Čl. 5. Uredbe (EZ) br. 767/2008 Europskog parlamenta i Vijeća od 9. srpnja 2008. o viznom informacijskom sustavu (VIS) i razmjeni podataka među državama članicama o vizama za kratkotrajni boravak (*Uredba o VIS-u*), SL 2008 L 218.

i Europol mogu zatražiti pristup podacima unesenim u sustav VIS radi sprečavanja, otkrivanja i istrage terorističkih i kaznenih djela.[281]

Eurodac

Naziv „Eurodac" odnosi se na daktilograme ili otiske prstiju. Radi se o centraliziranom sustavu s podacima o otiscima prstiju državljana trećih zemalja koji traže azil u jednoj od država članica Europske unije.[282] Sustav je u uporabi od siječnja 2003. i služi kao pomoć prilikom utvrđivanja koja bi država članica trebala biti odgovorna za razmatranje određenog zahtjeva za azil prema Uredbi Vijeća (EZ) br. 343/2003 o uvođenju kriterija i mehanizama za utvrđivanje države članice odgovorne za razmatranje zahtjeva za azil koji državljanin treće zemlje podnosi u jednoj od država članica (*Uredba Dublin II.*).[283] Osobne se podatke u Eurodacu može koristiti samo u svrhu omogućavanja primjene Uredbe Dublin II.; uporaba u bilo koju drugu svrhu je kažnjiva.

Sustav Eurodac sastoji se od središnje jedinice, kojom upravlja eu-LISA, za pohranu i usporedbu otisaka prstiju i sustava za elektronički prijenos podataka među državama članicama i središnjom bazom podataka. Države članice uzimaju i prenose otiske prstiju svake osobe koja nije državljanin Europske unije ili osobe bez državljanstva u dobi od najmanje 14 godina koja zatraži azil na njihovom području ili koja je uhićena radi neovlaštenog prelaska njihove vanjske granice. Države članice također mogu uzeti i prenijeti otiske prstiju osoba koje nisu državljani Europske unije ili osoba bez državljanstva unutar svojih područja bez dozvole.

Podaci o otiscima prstiju pohranjuju se u bazi podataka sustava Eurodac samo u pseudonimiziranom obliku. U slučaju podudaranja, pseudonim i ime prve države članice koja je prenijela podatke o otiscima prstiju otkriva se drugoj državi članici. Zatim se druga država članica obraća prvoj jer je, prema Uredbi Dublin II., prva država članica odgovorna za obradu zahtjeva za azil.

281 Vijeće Europske unije (2008), Odluka Vijeća 2008/633/PUP od 23. lipnja 2008. o pristupu određenih tijela država članica i Europola viznom informacijskom sustavu (VIS) za traženje podataka u svrhu sprečavanja, otkrivanja i istraga terorističkih kaznenih djela i ostalih teških kaznenih djela, SL 2008 L 218.

282 Uredba Vijeća (EZ) br. 2725/2000 od 11. prosinca 2000. o osnivanju sustava „Eurodac" za usporedbu otisaka prstiju za učinkovitu primjenu Dublinske konvencije, SL 2000 L 316; Uredba Vijeća (EZ) br. 407/2002 od 28. veljače 2002. o utvrđivanju određenih pravila za provedbu Uredbe (EZ) br. 2725/2000 o osnivanju sustava „Eurodac" za usporedbu otisaka prstiju za učinkovitu primjenu Dublinske konvencije, SL 2002 L 62 (*Uredba o Eurodacu*).

283 Uredba Vijeća (EZ) br. 343/2003 od 18. veljače 2003. o uvođenju kriterija i mehanizama za utvrđivanje države članice odgovorne za razmatranje zahtjeva za azil koji državljanin treće zemlje podnosi u jednoj od država članica, SL 2003 L 50 (*Uredba Dublin II.*).

Osobni podaci pohranjeni u sustavu Eurodac koji se odnose na tražitelje azila čuvaju se 10 godina od datuma uzimanja otisaka prstiju, osim ako osoba čiji se podaci obrađuju dobije državljanstvo države članice Europske unije. U tom se slučaju podaci moraju odmah izbrisati. Podaci koji se odnose na strane državljane uhićene zbog prelaska vanjske granice čuvaju se dvije godine. Ti se podaci moraju izbrisati čim osoba čiji se podaci obrađuju dobije dozvolu boravka, napusti područje Europske unije ili dobije državljanstvo države članice.

Osim svih država članica Europske unije, sustav Eurodac redovito koriste i Island, Norveška, Lihtenštajn i Švicarska.

Eurosur

Cilj je Europskog sustava za nadzor granica (*Eurosur*)[284] pojačati kontrolu vanjskih granica schengenskog prostora otkrivanjem, sprečavanjem i suzbijanjem nezakonite imigracije i prekograničnog kriminala. On služi za poboljšanje razmjene informacija i operativne suradnje između nacionalnih koordinacijskih centara i agencije Frontex Europske unije koja je zadužena za razvijanje i primjenu novog koncepta integriranog upravljanja granicama.[285] Njegovi su opći ciljevi:

- smanjiti broj nezakonitih migranata koji neotkriveni ulaze u Europsku uniju
- smanjiti broj smrti nezakonitih migranata spašavanjem većeg broja ljudi na moru
- povećati unutarnju sigurnost Europske unije u cjelini pomažući u sprečavanju prekograničnog kriminala.[286]

284 Uredba (EZ) br. 1052/2013 Europskog parlamenta i Vijeća od 22. listopada 2013. o osnivanju Europskog sustava za nadzor granica (Eurosur), SL L 2013 L 295.

285 Uredba (EU) br. 1168/2011 Europskog parlamenta i Vijeća od 25. listopada 2011. o izmjeni Uredbe Vijeća (EZ) br. 2007/2004 o osnivanju Europske agencije za upravljanje operativnom suradnjom na vanjskim granicama država članica Europske unije, SL 2011 L 394 (*Uredba o Frontrexu*).

286 Također vidjeti: Europska komisija (2008), Priopćenje Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija: Ispitivanje osnivanja Europskog sustava za nadzor granica (Eurosur), COM(2008) 68 završno, Bruxelles, 13. veljače 2008.; Europska komisija (2011), Procjena utjecaja uz Prijedlog uredbe Europskog parlamenta i Vijeća o osnivanju Europskog sustava za nadzor granica (Eurosur), Radni dokument službi Komisije, SEC(2011) 1536 završno, Bruxelles, 12. prosinca 2011., str. 18.

Počeo je djelovati od 2. prosinca 2013. u svim državama članicama s vanjskim granicama, a od 1. prosinca 2014. počet će djelovati i u drugima. Uredba će se primjenjivati na nadzor kopnenih, vanjskih morskih i zračnih granica država članica.

Carinski informacijski sustav

Još je jedan važan zajednički informacijski sustav uspostavljen na razini Europske unije – carinski informacijski sustav (CIS).[287] Tijekom uspostave unutarnjeg tržišta ukinute su sve kontrole i formalnosti vezane uz robu koja se kreće unutar područja Europske unije što je povećalo rizik od prijevare. Protuteža riziku je pojačana suradnja među carinskim upravama država članica. Svrha je CIS-a pomoći državama članicama u sprečavanju, istrazi i progonu teških kršenja carinskih i poljoprivrednih zakona na razini država i Europske unije.

Informacije iz CIS-a obuhvaćaju osobne podatke koji se odnose na zadržane, oduzete ili zaplijenjene proizvode, prijevozna sredstva, poduzeća, osobe, robu i gotovinu. Te se informacije mogu koristiti samo u svrhe opažanja, izvješćivanja ili izvršavanja određenih inspekcija ili u svrhe strateške ili operativne analize u vezi s osobama osumnjičenim za kršenje carinskih odredbi.

Pristup CIS-u dopušten je nacionalnim carinskim, poreznim, poljoprivrednim, javno-zdravstvenim i policijskim tijelima kao i Europolu i Eurojustu.

Obrada osobnih podataka mora biti u skladu s posebnim pravilima utvrđenim Uredbom br. 515/97 i Konvencijom o CIS-u,[288] kao i s odredbama Direktive o policijskim podacima, Uredbom o zaštiti podataka u institucijama Europske unije, Konvencijom br. 108 i Preporukom o policijskim podacima. Europski nadzornik za zaštitu podataka je odgovoran za nadzor ispunjava li CIS zahtjeve postavljene Uredbom (EZ) br. 45/2011 te barem jednom godišnje se sastaje s nacionalnim tijelima za zaštitu podataka država članica, koji su nadležni za nadzor obrade podataka u svezi s CIS-om.

287 Vijeće Europske unije (1995), Akt Vijeća od 26. srpnja 1995. o sastavljanju Konvencije o uporabi informacijske tehnologije u carinske svrhe, SL 1995 C 316, koju je izmijenilo Vijeće Europske unije (2009), Uredba br. 515/97 od 13. ožujka 1997. o uzajamnoj pomoći upravnih tijela država članica i o suradnji potonjih s Komisijom radi osiguravanja pravilne primjene propisa o carinskim i poljoprivrednim pitanjima, Odluka Vijeća 2009/917/PUP od 30. studenoga 2009. o uporabi informacijske tehnologije u carinske svrhe, SL 2009 L 323 (*Odluka o CIS-u*).

288 *Ibid.*

8

Ostali specifični zakonodavni propisi o zaštiti podataka

EU	Pitanja kojima se bavi	Vijeće Europe
Direktiva o zaštiti podataka Direktiva o privatnosti i elektroničkim komunikacijama	**Elektroničke komunikacije**	Konvencija br. 108 Preporuka o telekomunikacijskim uslugama
Direktiva o zaštiti podataka, članak 8. stavak 2. točka (b)	**Radni odnosi**	Konvencija br. 108 Preporuka o zapošljavanju ECtHR, *Copland protiv Ujedinjene Kraljevine*, br. 62617/00, 3. travnja 2007.
Direktiva o zaštiti podataka, članak 8. stavak 3.	**Medicinski podaci**	Konvencija br. 108 Preporuka o medicinskim podacima *ECtHR, Z. protiv Finske*, br. 22009/93, 25. veljače 1997.
Direktiva o kliničkim ispitivanjima	**Klinička ispitivanja**	
Direktiva o zaštiti podataka, članak 6. stavak 1. točke (b) i (e) i članak 13. stavak 2.	**Statistika**	Konvencija br. 108 Preporuka o statističkim podacima
Uredba (EZ) br. 223/2009 o europskoj statistici CJEU, C-524/06, *Huber protiv Njemačke*, 16. prosinca 2008.	**Službena statistika**	Konvencija br. 108 Preporuka o statističkim podacima

EU	Pitanja kojima se bavi	Vijeće Europe
Direktiva 2004/39/EZ o tržištima financijskih instrumenata Uredba (EU) br. 648/2012 o OTC izvedenicama, središnjoj drugoj ugovornoj strani i trgovinskom repozitoriju Uredba (EZ) br. 1060/2009 o agencijama za kreditni rejting Direktiva 2007/64/EZ o platnim uslugama na unutarnjem tržištu	**Financijski podaci**	Konvencija br. 108 Preporuka 90(19) koja se koristi za plaćanja i druge srodne aktivnosti ECtHR, *Michaud protiv Francuske*, br. 12323/11, 6. prosinca 2012.

U nekoliko su slučajeva na europskoj razini usvojeni posebni pravni instrumenti kojima se u određenim situacijama detaljnije primjenjuju opća pravila Konvencije br. 108 ili Direktive o zaštiti podataka.

8.1. Elektroničke komunikacije

Ključne točke

- Posebna pravila o zaštiti podataka u području telekomunikacija, s posebnim naglaskom na telefonske usluge, sadržana su u Preporuci Vijeća Europe iz 1995.
- Obrada osobnih podataka koji se odnose na pružanje komunikacijskih usluga na razini Europske unije uređena je Direktivom o privatnosti i elektroničkim komunikacijama.
- Povjerljivost elektroničkih komunikacija odnosi se ne samo na sadržaj komunikacije, već i na podatke o prometu, kao što su informacije o tome tko je komunicirao s kime, kad se komunikacija odvijala i koliko dugo je trajala, kao i na podatke o lokaciji, kao što je lokacija s koje su podaci priopćeni.

U komunikacijskim je mrežama veća mogućnost neopravdanog miješanja u osobnu sferu korisnika zbog dodatnih tehničkih mogućnosti prisluškivanja i praćenja komunikacije koja se odvija na takvim mrežama. Zbog toga se smatralo da su potrebni posebni propisi o zaštiti podataka radi sprečavanja određenih rizika kojima su izloženi korisnici komunikacijskih usluga.

Vijeće Europe izdalo je 1995. godine Preporuku o zaštiti podataka u području telekomunikacija koja se naročito odnosila na telefonske usluge.[289] Prema toj preporuci, svrhe prikupljanja i obrade osobnih podataka u kontekstu telekomunikacija treba ograničiti na: spajanje korisnika na mrežu, ponudu određene telekomunikacijske usluge, naplatu, provjeru, osiguravanje optimalnog tehničkog rada i razvoj mreže i usluge.

Posebna je pažnja posvećena i uporabi telekomunikacijskih mreža za slanje poruka direktnog marketinga. Poruke direktnog marketinga u pravilu ne smiju biti usmjerene ni na kojeg pretplatnika koji je izričito izjavio da ne želi primati promidžbene poruke. Uređaji za automatsko pozivanje koji prenose unaprijed snimljene promidžbene poruke smiju se koristiti samo ako je pretplatnik dao svoju izričitu suglasnost za to. Nacionalnim zakonodavstvom treba propisati detaljna pravila u tom području.

Što se tiče **pravnog okvira Europske unije,** nakon prvog pokušaja 1997., Direktiva o privatnosti i elektroničkim komunikacijama usvojena je 2002. i izmijenjena 2009. radi nadopunjavanja i specificiranja odredbi Direktive o zaštiti podataka za telekomunikacijski sektor.[290] Primjena Direktive o privatnosti i elektroničkim komunikacijama ograničena je na komunikacijske usluge u javnim elektroničkim mrežama.

Direktiva o privatnosti i elektroničkim komunikacijama razlikuje tri glavne vrste podataka nastalih pri komuniciranju:

- podaci koji čine sadržaj poruka poslanih tijekom komuniciranja; ti su podaci strogo povjerljivi

- podaci potrebni za uspostavu i održavanje komunikacije, takozvani podaci o prometu, kao što su informacije o osobama koje komuniciraju, vremenu i trajanju komunikacije

289 CoE, Odbor ministara (1995), Preporuka Rec(95)4 državama članicama o zaštiti osobnih podataka u području telekomunikacijskih usluga, s posebnim naglaskom na telefonske usluge, 7. veljače 1995.

290 Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u sektoru elektroničkih komunikacija, SL 2002 L 201 (*Direktiva o privatnosti i elektroničkim komunikacijama*), kako je izmijenjena Direktivom 2009/136/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o izmjeni Direktive 2002/22/EZ o univerzalnoj usluzi i pravima korisnika u vezi s elektroničkim komunikacijskim mrežama i uslugama, Direktiva 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u sektoru elektroničkih komunikacija i Uredba (EZ) br. 2006/2004 o suradnji nacionalnih tijela za provedbu zakona o zaštiti potrošača, SL 2009 L 337.

- podaci o prometu, koji obuhvaćaju podatke koji se posebno odnose na lokaciju komunikacijskog uređaja, takozvane podatke o lokaciji; ti su podaci istovremeno podaci o lokaciji *korisnika* komunikacijskih uređaja i naročito su bitni u pogledu korisnika mobilnih komunikacijskih uređaja.

Podatke o prometu može koristiti pružatelj usluge za potrebe naplate usluge i za tehničko pružanje usluge. Međutim, uz suglasnost osobe čiji se podaci obrađuju, ti se podaci mogu otkriti drugim nadzornicima koji pružaju usluge dodane vrijednosti, kao što je pružanje informacija vezanih uz lokaciju korisnika, o sljedećem stajalištu podzemne željeznice ili ljekarne ili vremenske prognoze za tu lokaciju.

Ostali pristupi podacima o komunikacijama u elektroničkim mrežama, kao što je pristup u svrhu istrage kriminala, prema članku 15. Direktive o privatnosti i elektroničkim komunikacijama, moraju ispunjavati zahtjeve za opravdanim miješanjem u pravo na zaštitu podataka kako je navedeno u članku 8. stavku 2. Europske konvencije o ljudskim pravima i potvrđeno u člancima 8. i 52. Povelje.

Izmjenama Direktive o privatnosti i elektroničkim komunikacijama iz 2009.[291] uvedeno je sljedeće:

- Ograničenja slanja e-pošte u svrhu direktnog marketinga proširena su na usluge kratkih (SMS) poruka, usluge multimedijskih poruka i ostale vrste sličnih aplikacija; promidžbena e-pošta zabranjena je osim uz prethodnu suglasnost. Bez takve suglasnosti dopušteno je obraćanje promidžbenom e-poštom samo bivšim kupcima ako su ostavili svoje adrese e-pošte nemaju primjedbi na takvo obraćanje.

- Državama članicama nametnuta je obveza pružanja pravnih lijekova protiv kršenja zabrane neželjene komunikacije.[292]

- Postavljanje kolačića, softvera koji nadzire i snima aktivnosti korisnika računala više nije dopušteno bez suglasnosti korisnika računala. Nacionalnim

291 Direktiva 2009/136/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o izmjeni Direktive 2002/22/EZ o univerzalnoj usluzi i pravima korisnika u vezi s elektroničkim komunikacijskim mrežama i uslugama, Direktiva 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u sektoru elektroničkih komunikacija i Uredba (EZ) br. 2006/2004 o suradnji nacionalnih tijela za provedbu zakona o zaštiti potrošača, SL 2009 L 337.

292 Vidjeti izmijenjenu Direktivu, čl. 13.

zakonodavstvom treba detaljnije urediti način na koji treba izjaviti i pribaviti suglasnost radi osiguravanja odgovarajuće razine zaštite.[293]

Ako je do povrede podataka došlo zbog neovlaštenog pristupa, gubitka ili uništavanja podataka, o tome je potrebno odmah obavijestiti nadležno nadzorno tijelo. Pretplatnike treba obavijestiti ako je šteta koju su eventualno pretrpjeli posljedica povrede podataka.[294]

Prema Direktivi o zadržavanju podataka[295] (proglašena nevaljanom 8. travnja 2014.) pružatelji komunikacijskih usluga dužni su staviti na raspolaganje podatke o prometu, posebno u svrhu suzbijanja teškog kriminala, tijekom razdoblja od najmanje šest mjeseci i ne dužeg od 24 mjeseca, bez obzira na to jesu li pružatelju ti podaci i dalje bili potrebni u svrhu naplate ili tehničkog pružanja usluge.

Države članice Europske unije imenuju neovisna javna tijela odgovorna za nadzor sigurnosti zadržanih podataka.

Jasno je da zadržavanje telekomunikacijskih podataka zadire u pravo na zaštitu podataka.[296] U nekoliko sudskih postupaka provedenih u državama članicama Europske unije razmatralo se je li takvo zadiranje opravdano.[297]

Primjer: U predmetu *Digital Rights Ireland i Seitlinger i drugi,*[298] CJEU je proglasio Direktivu o zadržavanju podataka nevaljanom. Prema shvaćanju Suda, „široko i posebno ozbiljno zadiranje Direktive u temeljna prava u pitanju, nije dovoljno

293 Vidjeti *Ibid.*, čl. 5.; vidjeti i *Mišljenje 04/2012 Radne skupine iz članka 29. (2012) o izuzeću u vezi sa suglasnosti za kolačiće*, WP 194, Bruxelles, 7. lipnja 2012.

294 Vidjeti također *Radni dokument 01/2011* Radne skupine iz članka 29. (2011) *o trenutačnom okviru Europske unije za povredu osobnih podataka i preporukama za budući razvoj politike*, WP 184, Bruxelles, 5. travnja 2011.

295 Direktiva 2006/24/EZ Europskog parlamenta i Vijeća od 15. ožujka 2006. o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža i o izmjeni Direktive 2002/58/EZ, SL L 2006 L 105.

296 EDPS (2011), *Mišljenje od 31. svibnja 2011. o evaluacijskom izvješću Komisije Vijeću i Europskom parlamentu o Direktivi o zadržavanju podataka (Direktiva 2006/24/EZ)*, 31. svibnja 2011.

297 Njemačka, Savezni ustavni sud (*Bundesverfassungsgericht*), 1 BvR 256/08, 2. ožujka 2010.; Rumunjska, Savezni ustavni sud (*Curtea Constituțională a României*), br. 1258, 8. listopada 2009.; Republika Češka, Ustavni sud (*Ústavní soud České republiky*), 94/2011 Coll., 22. ožujka 2011.

298 CJEU, zajednički predmeti C-293/12 i C-594/12 *Digital Rights Ireland i Seitlinger i drugi,* I8. travnja 2014., odlomak 65.

ograničeno kako bi se osiguralo da to zadiranje bude u najmanjem mogućem opsegu potrebnom za postizanje svrhe".

Miješanje javnih tijela najveći je problem u kontekstu elektroničkih komunikacija. Sredstva za nadziranje ili presretanje komunikacija, kao što su prislušni uređaji ili uređaji za prisluškivanje, dopuštena su samo ako su propisana zakonom i ako predstavljaju mjeru nužnu u demokratskom društvu u interesu: zaštite državne sigurnosti, javne sigurnosti, novčanih interesa države ili suzbijanja kaznenih djela; ili zaštite osobe čiji se podaci obrađuju ili prava i sloboda drugih.

Primjer: U predmetu Malone protiv Ujedinjene Kraljevine[299] podnositelj je optužen za niz kaznenih djela u vezi s nepoštenim postupanjem s ukradenom robom. Tijekom suđenja pokazalo se da je telefonski razgovor podnositelja presretan na temelju naloga koji je Ministar unutarnjih poslova izdao za Ministarstva unutarnjih poslova. Iako je način na koji je podnositeljeva komunikacija presretana bio zakonit u smislu nacionalnog zakonodavstva, Europski sud za ljudska prava smatrao je da nije bilo zakonskih pravila koja uređuju opseg i način na koji javna tijela ostvaruju svoja diskrecijska prava u tom području te da miješanje koje je rezultat predmetne prakse stoga nije bilo „u skladu sa zakonom." Sud je smatrao da je prekršen članak 8. Konvencije.

8.2. Podaci o zaposlenju

Ključne točke

- Posebna pravila o zaštiti podataka u radnim odnosima sadržana su u Preporuci o podacima o zaposlenju Vijeća Europe.
- U Direktivi o zaštiti podataka, radni odnosi spominju se konkretno samo u kontekstu obrade osjetljivih podataka.
- Valjanost suglasnosti, koja mora dobrovoljna, kao pravne osnove za obradu podataka o zaposlenicima može biti dvojbena s obzirom na ekonomsku neravnotežu između poslodavca i zaposlenika. Okolnosti davanja suglasnosti moraju se pažljivo procijeniti.

U Europskoj uniji ne postoji poseban pravni okvir kojim se uređuje obrada podataka u kontekstu zaposlenja. U Direktivi o zaštiti podataka, radni odnosi spominju se konkretno samo u članku 8. stavku 2. Direktive koji se bavi obradom osjetljivih

299 ECtHR, *Malone protiv Ujedinjene Kraljevine*, br. 8691/79, 26. travnja 1985.

podataka. Što se tiče Vijeća Europe, Preporuka o podacima o zaposlenju izdana je 1989. i trenutačno se ažurira.[300]

Pregled najčešćih problema u vezi sa zaštitom podataka u konkretnom kontekstu zaposlenja nalazi se u radnom dokumentu Radne skupine iz članka 29.[301] Radna je skupina analizirala važnost suglasnosti kao pravne osnove za obradu podataka o zaposlenju.[302] Radna je skupina utvrdila da će zbog ekonomske neravnoteže između poslodavca koji traži suglasnost i zaposlenika koji daje suglasnost uvijek biti dvojbeno je li suglasnost dobrovoljna. Stoga pri procjeni valjanosti suglasnosti u kontekstu zaposlenja valja pažljivo razmotriti okolnosti davanja suglasnosti.

Čest problem vezan uz zaštitu podataka u tipičnom današnjem radnom okruženju jest legitiman opseg nadzora elektroničkih komunikacija zaposlenika na radnom mjestu. Često se tvrdi da se taj problem može lako riješiti zabranom privatne uporabe komunikacijskih sredstava na radnom mjestu. Međutim, takva bi opća zabrana mogla biti nerazmjerna i nerealna. Sljedeća je presuda Europskog suda za ljudska prava naročito bitna u ovom kontekstu:

Primjer: U predmetu *Copland protiv Ujedinjene Kraljevine*,[303] tajno su nadzirani telefon, e-pošta i uporaba interneta zaposlenice više škole kako bi se utvrdilo koristi li prekomjerno školska sredstva u osobne svrhe. Europski sud za ljudska prava smatrao je da su telefonski pozivi iz poslovnih prostorija obuhvaćeni pojmovima privatnog života i dopisivanja. Stoga su takvi pozivi i e-pošta poslani s radnog mjesta, kao i informacije dobivene na temelju nadzora osobne uporabe interneta zaštićeni člankom 8. Europske konvencije o ljudskim pravima. U slučaju podnositeljice nisu postojale odredbe kojima se uređuju okolnosti u kojima poslodavci mogu nadzirati zaposlenikovu uporabu telefona, e-pošte i interneta. Stoga miješanje nije bilo u skladu sa zakonom. Sud je zaključio da je prekršen članak 8. Konvencije.

300 Vijeće Europe, Odbor ministara (1989), Preporuka Rec(89)2 državama članicama o zaštiti osobnih podataka koji se koriste u svrhu zaposlenja, 18. siječnja 1989. Vidjeti dodatno Savjetodavni odbor uz Konvenciju br. 108, Studija preporuke br. R (89) 2 o zaštiti osobnih podataka koji se koriste u svrhu zaposlenja i o prijedlozima za reviziju spomenute Preporuke, 9. rujna 2011.

301 *Mišljenje 8/2001 o obradi osobnih podataka u kontekstu zaposlenja* Radne skupine iz članka 29. (2001.), WP 48, Bruxelles, 13. rujna 2001.

302 Radna skupina iz članka 29. (2005), *Radni dokument o zajedničkom tumačenju članka 26. stavka 1. Direktive 95/46/EZ od 24. listopada 1995.*, WP 144, Bruxelles, 25. studenoga 2005.

303 ECtHR, *Copland protiv Ujedinjene Kraljevine*, br. 62617/00, 3. travnja 2007.

Prema preporuci Vijeća Europe o zaposlenju, osobne podatke koji se prikupljaju u svrhu zaposlenja treba dobiti izravno od pojedinog zaposlenika.

Osobni podaci koji se prikupljaju radi zapošljavanja moraju se ograničiti na informacije koje su potrebne za procjenu prikladnosti kandidata i njihova radnog potencijala.

U preporuci se također posebno spominju podaci o mišljenju o učinkovitosti ili potencijalu pojedinih zaposlenika. Podaci o mišljenju moraju se temeljiti na poštenim i pravednim ocjenama i ne smiju biti formulirani na uvredljiv način. To je uvjetovano načelima poštene obrade podataka i točnosti podataka.

Poseban je vid zakonodavstva o zaštiti podataka u odnosu između zaposlenika i poslodavca uloga predstavnika zaposlenika. Predstavnici smiju primati osobne podatke o zaposlenicima samo ako je to potrebno da bi mogli zastupati interese zaposlenika.

Osjetljivi osobni podaci koji se prikupljaju u svrhe zaposlenja smiju se obrađivati samo u određenim slučajevima i u skladu sa zaštitnim mjerama koje propisuje nacionalno zakonodavstvo. Poslodavci mogu zaposlenike ili kandidate za posao pitati o njihovu zdravstvenom stanju ili ih podvrgnuti zdravstvenom pregledu samo ako je to potrebno kako bi: utvrdili njihovu prikladnost za radno mjesto; ispunili zahtjeve preventivne medicine; ili kako bi se odobrila socijalna davanja. Zdravstveni se podaci smiju prikupljati samo od dotičnog zaposlenika, a ne iz drugih izvora, osim uz izričitu i informiranu suglasnost ili ako je to propisano nacionalnim zakonodavstvom.

U skladu s Preporukom o zaposlenju, zaposlenici trebaju biti informirani o svrsi obrade njihovih osobnih podataka, vrsti pohranjenih osobnih podataka, tijelima kojima se podaci redovito priopćuju i svrsi i pravnoj osnovi takvih priopćenja. Poslodavci bi također svoje zaposlenike trebali unaprijed obavijestiti o uvođenju ili prilagodbi automatiziranih sustava za obradu osobnih podataka zaposlenika ili za nadzor kretanja ili produktivnosti zaposlenika.

Zaposlenici moraju imati pravo na pristup svojim podacima o zaposlenju kao i pravo na njihov ispravak ili brisanje. Ako se obrađuju podaci o mišljenju, zaposlenici moraju imati pravo osporiti mišljenje. Međutim, ta prava mogu biti privremeno ograničena u svrhu unutarnjih istraga. Ako se zaposleniku odbije pristup, ispravak ili brisanje osobnih podataka o zaposlenju, nacionalnim zakonodavstvom moraju se propisati odgovarajući postupci kojima se osporava takvo odbijanje.

8.3. Medicinski podaci

Ključne točke

- Medicinski podaci su osjetljivi, stoga uživaju posebnu zaštitu.

Osobni podaci u vezi sa zdravstvenim stanjem osobe čiji se podaci obrađuju smatraju se osjetljivim podacima prema članku 8. stavku 1. Direktive o zaštiti podataka i članku 6. Konvencije br. 108. Stoga medicinski podaci podliježu strožem režimu obrade podataka od neosjetljivih podataka.

Primjer: U predmetu *Z. protiv Finske*,[304] bivši suprug podnositeljice, koji je bio zaražen virusom HIV-a, počinio je niz spolnih kaznenih djela. Kasnije je osuđen za ubojstvo jer je svoje žrtve svjesno izložio riziku od zaraze HIV-om. Nacionalni je sud naložio da cjelokupna presuda i dokumenti iz predmeta ostanu povjerljivi 10 godina unatoč zahtjevima podnositeljice za dužim razdobljem povjerljivosti. Te je zahtjeve odbio prvostupanjski sud čija je presuda sadržavala puna imena i podnositeljice i njezina bivšeg supruga. Europski sud za ljudska prava smatrao je da miješanje nije bilo nužno u demokratskom društvu jer je zaštita medicinskih podataka od temeljne važnosti za ostvarenje prava na poštovanje privatnog i obiteljskog života, naročito kad se radi o informacijama o zarazi HIV-om, jer je to stanje stigmatizirano u mnogim društvima. Stoga je Sud zaključio da bi se odobravanjem pristupa podnositeljevu identitetu i zdravstvenom stanju, kako je opisano u presudi prvostupanjskog suda po isteku razdoblja od 10 godina nakon donošenja presude, prekršio članak 8. Europske konvencije o ljudskim pravima.

Člankom 8. stavkom 3. Direktive o zaštiti podataka omogućena je obrada medicinskih podataka potrebnih radi preventivne medicine, zdravstvene dijagnoze, pružanja skrbi ili liječenja ili u svrhu upravljanja zdravstvenim uslugama. Međutim, obrada je dopuštena samo ako je provodi zdravstveni radnik koji ima obvezu čuvanja poslovne tajne ili druga osoba koja ima istu tu obvezu.[305]

304 *ECtHR, Z. protiv Finske*, br. 22009/93, 25. veljače 1997., st. 94. i 112.; vidjeti također ECtHR, *M.S. protiv Švedske*, br. 20837/92, 27. kolovoza 1997., *L.L. protiv Francuske*, br. 7508/02, 10. listopada 2006.; ECtHR, *I. protiv Finske*, br. 20511/03, 17. srpnja 2008.; ECtHR, *K.H. i drugi protiv Slovačke*, br. 32881/04, 28. travnja 2009.; ECtHR, *Szuluk protiv Ujedinjene Kraljevine*, br. 36936/05, 2 ipnja 2009.

305 Vidjeti također ECtHR, *Biriuk protiv Litve*, br. 23373/03, 25. studenog 2008.

U Preporuci Vijeća Europe o medicinskim podacima iz 1997. na obradu podataka u području medicine detaljnije se primjenjuju načela Konvencije br. 108.[306] Predložena su pravila u skladu s onima iz Direktive o zaštiti podataka u pogledu zakonitih svrha obrade medicinskih podataka, obveza čuvanja poslovne tajne osoba koje koriste medicinske podatke, i prava osoba čiji se podaci obrađuju na transparentnost i pristup, ispravak i brisanje. Osim toga, medicinski podaci koje zdravstveni radnici zakonito obrađuju ne smiju se prenijeti tijelima za provedbu zakona ako nisu osigurane „odgovarajuće zaštitne mjere kojima se sprečava otkrivanje koje nije u skladu s pravom na poštovanje [...] privatnog života koje je zajamčeno člankom 8. Europske konvencije o ljudskim pravima".[307]

Osim toga, Preporuka o medicinskim podacima sadrži posebne odredbe o medicinskim podacima nerođene djece i nemoćnim osobama, kao i o obradi genetičkih podataka. Znanstvena su istraživanja izričito priznata kao razlog za čuvanje podataka duže nego što su potrebni, iako je to najčešće zahtijeva anonimizaciju. U članku 12. Preporuke o medicinskim podacima predlažu se detaljni propisi za situacije u kojima su istraživačima potrebni osobni podaci, a anonimizirani podaci nisu dovoljni.

Pseudonimizacija može biti dobar način za ispunjavanje znanstvenih potreba i zaštitu interesa pacijenata. U odjeljak 2.1.3 detaljnije se objašnjava načelo pseudonimizacije u kontekstu zaštite podataka.

Na nacionalnoj i europskoj razini provode se intenzivne rasprave o inicijativama pohrane podataka o medicinskom liječenju pacijenta u elektroničkom zdravstvenom kartonu.[308] Poseban aspekt nacionalnih sustava elektroničkih zdravstvenih kartona jest njihova dostupnost preko granice: tema od posebnog značaja unutar Europske unije u kontekstu prekogranične zdravstvene skrbi.[309]

Druga su tema rasprave vezane uz nove odredbe klinička ispitivanja, drugim riječima, isprobavanje novih lijekova na pacijentima u dokumentiranom istraživačkom okruženju; ta je tema također u mnogočemu povezana sa zaštitom podataka. Klinička ispitivanja lijekova za humanu uporabu regulirana su Direktivom 2001/20/EZ

306 CoE, Odbor ministara (1997), Preporuka Rec(97)5 državama članicama o zaštiti medicinskih podataka, 13. veljače 1997.

307 ECtHR, *Avilkina i drugi protiv Rusije*, br. 1585/09, 6. lipnja 2013., st. 53. (nije završno).

308 Radna skupina iz članka 29. (2007.), *Radni dokument o obradi osobnih podataka vezanih uz zdravlje u elektroničkim zdravstvenim kartonima (EHR)*, WP 131, Bruxelles, 15. veljače 2007.

309 Direktiva Europskog parlamenta i Vijeća 2011/24/EU od 9. ožujka 2011. o primjeni prava pacijenata u prekograničnoj zdravstvenoj skrbi, SL 2011 L 88.

Europskog parlamenta i Vijeća od 4. travnja 2001. o usklađivanju zakonodavstava i drugih propisa država članica koji se odnose na provedbu dobre kliničke prakse prilikom provođenja kliničkih ispitivanja lijekova za humanu uporabu (*Direktiva o kliničkim ispitivanjima*).[310] U prosincu 2012. Europska komisija predložila je uredbu kojom bi se zamijenila Direktiva o kliničkim ispitivanjima kako bi postupci ispitivanja bili ujednačeniji i učinkovitiji.[311]

Na razini Europske unije u tijeku je još mnogo drugih zakonodavnih i drugih inicijativa vezanih uz osobne podatke u zdravstvenom sektoru.[312]

8.4. Obrada podataka u statističke svrhe

Ključne točke

- Podaci koji se prikupljaju u statističke svrhe ne smiju se koristiti ni u koju drugu svrhu.
- Podaci koji se zakonito prikupljaju u bilo koju svrhu mogu se dalje koristiti u statističke svrhe pod uvjetom da su nacionalnim zakonodavstvom propisane odgovarajuće zaštitne mjere koje korisnici primjenjuju. Zbog toga svakako treba predvidjeti anonimizaciju ili pseudonimizaciju prije prijenosa trećim strankama.

U Direktivi o zaštiti podataka obrada podataka u statističke svrhe spominje se u kontekstu mogućih izuzeća od načela zaštite podataka. Prema članku 6. stavku 1. točki (b) Direktive, nacionalnim se zakonodavstvom može odbaciti načelo ograničenja svrhe u korist daljnje uporabe podataka u statističke svrhe, no nacionalnim se zakonodavstvom moraju propisati i potrebne zaštitne mjere. Prema članku 13. stavku 2. Direktive, moguće je nacionalnim zakonodavstvom ograničiti prava na pristup ako se podaci obrađuju isključivo u statističke svrhe; no nacionalnim se zakonodavstvom i u tom slučaju moraju propisati odgovarajuće zaštitne mjere. U tom se kontekstu Direktivom o zaštiti podataka propisuje poseban zahtjev da se podaci

310 Direktiva 2001/20/EZ Europskog parlamenta i Vijeća od 4. travnja 2001. o usklađivanju zakonodavstava i drugih propisa država članica koji se odnose na provedbu dobre kliničke prakse prilikom provođenja kliničkih ispitivanja lijekova za humanu uporabu, SL 2001 L 121.

311 Europska komisija (2012), *Prijedlog uredbe Europskog parlamenta i Vijeća o kliničkim ispitivanjima medicinskih proizvoda za humanu uporabu i stavljanju izvan snage Direktive 2001/20/EZ*, COM(2012), 369 završno, Bruxelles, 17. srpnja 2012.

312 EDPS (2013), *Mišljenje Europskog nadzornika za zaštitu podataka o priopćenju Komisije o „Akcijskom planu za e-zdravstvo za razdoblje od 2012. - 2020. - Inovativno zdravstvo za 21. stoljeće"*, Bruxelles, 27. ožujka 2013.

dobiveni ili nastali tijekom statističkog istraživanja ne smiju koristiti za konkretne odluke o osobama čiji se podaci obrađuju.

Iako podatke koje je zakonito prikupio u bilo koju svrhu nadzornik može ponovno koristiti u vlastite statističke svrhe – za takozvanu sekundarnu statistiku – podatke treba anonimizirati ili pseudonimizirati, ovisno o slučaju, prije njihova prenošenja trećoj stranki u statističke svrhe, osim ako je osoba čiji se podaci obrađuju za to dala svoju suglasnost ili ako je to posebno propisano nacionalnim zakonodavstvom. To proizlazi iz zahtjeva za odgovarajućim zaštitnim mjerama prema članku 6. stavku 1. točki (b) Direktive o zaštiti podataka.

Najvažniji slučajevi uporabe podataka u statističke svrhe jesu službene statistike koje provode nacionalni zavodi za statistiku i zavodi za statistiku Europske unije na temelju nacionalnih zakonodavstava i zakonodavstva Europske unije o službenoj statistici. Prema tim zakonodavstvima, građani i poduzeća uglavnom su dužni otkriti podatke tijelima nadležnim za statistiku. Službenici koji rade u zavodima za statistiku dužni su čuvati poslovnu tajnu. Tu svoju dužnost moraju pažljivo ispunjavati kako bi građani imali visoku razinu povjerenja te stavili svoje podatke na raspolaganje tijelima nadležnim za statistiku.

U Uredbi (EZ) br. 223/2009 o europskoj statistici (*Uredba o europskoj statistici*) sadržana su osnovna pravila za zaštitu podataka u službenoj statistici koja se, dakle, mogu smatrati bitnima i za odredbe o službenoj statistici na nacionalnoj razini.[313] U Uredbi se zastupa načelo da je za službene statističke aktivnosti potrebna dovoljno precizna pravna osnova.[314]

> Primjer: U predmetu *Huber protiv Njemačke*,[315] Sud Europske unije utvrdio je da prikupljanje i pohrana osobnih podataka koje nadležno tijelo provodi u statističke svrhe sami po sebi nisu dovoljni da bi se obrada smatrala zakonitom.

313 Uredba (EZ) br. 223/2009 o europskoj statistici i stavljanju izvan snage Uredbe (EZ, Euratom) br. 1101/2008 Europskog parlamenta i Vijeća o dostavi povjerljivih statističkih podataka Statističkom uredu Europskih zajednica, Uredbe Vijeća (EZ) br. 322/97 o statistici Zajednice i Odluke Vijeća 89/382/EEZ, Euratom o osnivanju Odbora za statistički program Europskih zajednica, SL 2009 L 87.

314 Načelo će se dalje razraditi u Eurostatovom Kodeksu prakse koji će, u skladu s člankom 11. Uredbe o europskoj statistici, navoditi etičke smjernice o načinu provedbe službene statistike, uključujući pažljivu uporabu osobnih podataka. Dostupno na adresi: http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

315 CJEU, C-524/06, *Huber protiv Njemačke*, 16. prosinca 2008.; vidjeti posebno st. 68.

Zakonodavstvo kojim se propisuje obrada osobnih podataka također je trebalo ispuniti zahtjev nužnosti, što u danom kontekstu nije bio slučaj.

U kontekstu Vijeća Europe, Preporuka o statističkim podacima koja je izdana 1997. koja pokriva provedbu statistike u javnom i privatnom sektoru.[316] Tom se preporukom uvode načela koja se podudaraju s gore opisanim glavnim pravilima Direktive o zaštiti podataka. U vezi sa sljedećim pitanjima navedena su detaljnija pravila.

Dok se podaci koje je prikupio nadzornik u statističke svrhe ne mogu koristiti ni u koju drugu svrhu, podaci prikupljeni u svrhe koje nisu statističke prirode moraju biti raspoloživi za daljnju uporabu u statističke svrhe. Preporukom o statističkim podacima čak je dozvoljeno priopćavanje podataka trećim strankama ako se to čini samo u statističke svrhe. U tim bi slučajevima stranke trebale dogovoriti i zabilježiti opseg zakonite daljnje uporabe u statističke svrhe. Budući da to ne zamjenjuje suglasnost osobe čiji se podaci obrađuju, za pretpostaviti je da u nacionalnom zakonodavstvu moraju biti propisane dodatne zaštitne mjere radi smanjenja rizika od zlouporabe osobnih podataka, kao što je obveza anonimizacije ili pseudonimizacije podataka prije prijenosa.

Osobe koje se profesionalno bave statističkim istraživanjem trebaju biti dužne poštovati obvezu čuvanja poslovne tajne - kao što je to uobičajeno kod službene statistike – na temelju nacionalnog zakonodavstva. To treba proširiti i na ispitivače ako su zaposleni na prikupljanju podataka od osoba čiji se podaci obrađuju ili drugih osoba.

Ako uporaba podataka u statističkom istraživanju nije propisana zakonom, osobe čiji se podaci obrađuju trebaju dati suglasnost za uporabu svojih podataka ili barem imati mogućnost prigovora kako bi obrada bila zakonita. Ako ispitivači prikupljaju osobne podatke u statističke svrhe, te osobe moraju biti jasno informirane o tome je li otkrivanje podataka obvezno prema nacionalnom zakonodavstvu. Osjetljive se podatke nikad ne smije prikupljati na način da se pojedinac može identificirati, osim ako je to izričito dozvoljeno nacionalnim zakonodavstvom.

Ako statističko istraživanje nije moguće provesti s anonimiziranim podacima, i ako su osobni podaci doista nužni, podatke prikupljene u tu svrhu treba anonimizirati što je prije moguće. Na temelju rezultata statističkog istraživanja u najmanju ruku ne smije

316 Vijeće Europe, Odbor ministara (1997), Preporuka Rec(97)18 državama članicama o zaštiti osobnih podataka koji se prikupljaju i obrađuju u statističke svrhe, 30. rujna 1997.

biti moguće identificirati osobe čiji se podaci obrađuju, osim ako to jasno ne predstavlja nikakav rizik.

Po završetku statističke analize osobne podatke treba ili izbrisati ili anonimizirati. U tom je slučaju u Preporuci o statističkim podacima predložena pohrana identifikacijskih podataka odvojeno od ostalih osobnih podataka. To na primjer znači da podatke treba pseudonimizirati, a ključ za kodiranje ili popis sinonima za identifikaciju pohraniti odvojeno od pseudonimiziranih podataka.

8.5. Financijski podaci

Ključne točke

- Iako financijski podaci nisu osjetljivi podaci u smislu Konvencije br. 108 ili Direktive o zaštiti podataka, za njihovu su obradu potrebne posebne zaštitne mjere radi osiguravanja točnosti i sigurnosti podataka.
- Elektronički platni sustavi zahtijevaju ugrađenu zaštitu podataka, takozvanu ugrađenu privatnost.
- U tom području dolazi do određenih problema sa zaštitom podataka, jer treba primjenjivati odgovarajuće mehanizme za autentikaciju.

Primjer: U predmetu *Michaud protiv Francuske*,[317] podnositelj, francuski odvjetnik, suprotstavio se svojoj obvezi prijave sumnji vezanih uz moguće aktivnosti pranja novca koje provode njegovi klijenti, na što ga je obvezivalo francusko zakonodavstvo. Europski sud za ljudska prava smatrao je da je zahtijevanje od odvjetnika da upravnim tijelima prijavljuju informacije koje se odnose na drugu osobu, a koje su dobili kroz razmjenu informacija s tom osobom, predstavlja miješanje u pravo odvjetnika na poštovanje njihove korespondencije i privatnog života prema članku 8. Europske konvencije o ljudskim pravima jer to načelo obuhvaća aktivnosti profesionalne ili poslovne prirode. Međutim, miješanje je bilo u skladu sa zakonom i imalo je legitimnu svrhu, točnije spriječiti nered i kriminal. Budući da odvjetnici podliježu obvezi prijavljivanja sumnji samo

317 ECtHR, *Michaud protiv Franceuske*, br. 12323/11, 6. prosinca 2012.; vidjeti također ECtHR, *Niemietz protiv Njemačke*, br. 13710/88, 16. prosinca 1992., st. 29., i ECtHR, *Halford protiv Ujedinjene Kraljevine*, br. 20605/92, 25. lipnja 1997., st. 42.

u vrlo ograničenim okolnostima, Europski sud za ljudska prava smatrao je da je ta obveza razmjerna i zaključio da nije prekršen članak 8.

Primjenu općeg okvira za zaštitu podataka iz Konvencije br. 108 na kontekst plaćanja razradilo je Vijeće Europe u Preporuci Rec(90)19 iz 1990.[318] U toj je preporuci razjašnjen opseg zakonitog prikupljanja i uporabe u kontekstu plaćanja, naročito platnim karticama. U njoj se nadalje nacionalnim zakonodavcima predlažu detaljni propisi o ograničenjima u pogledu priopćavanja podataka o plaćanju trećim strankama, o vremenskim ograničenjima za zadržavanje podataka, o transparentnosti, sigurnosti podataka i prekograničnom prijenosu podataka i, naposljetku, o nadzoru i pravnim lijekovima. Predložena rješenja podudaraju se s kasnije propisanim općim okvirom za zaštitu podataka Europske unije u Direktivi o zaštiti podataka.

U izradi je niz pravnih instrumenata za uređenje tržišta financijskih instrumenata i aktivnosti kreditnih institucija i investicijskih društava.[319] Ostali pravni instrumenti pomažu u suzbijanju trgovanja na temelju povlaštenih informacija i manipuliranja tržištem.[320] Najvažnija su pitanja u tim područjima koja utječu na zaštitu podataka:

- zadržavanje zapisa o financijskim transakcijama
- prijenos osobnih podataka u treće zemlje
- snimanje telefonskih razgovora ili elektroničke komunikacije, uključujući ovlaštenje nadležnih tijela da zatraže zapise o telefonskom i podatkovnom prometu

318 CoE, Odbor ministara (1990), Preporuka br. R(90) 19 o zaštiti osobnih podataka korištenih za plaćanje i druge srodne radnje, 13. rujna 1990.

319 Europska komisija (2011), *Prijedlog direktive Europskog parlamenta i Vijeća o tržištima financijskih instrumenata i stavljanju izvan snage Direktive 2004/39/EZ Europskog parlamenta i Vijeća*, COM(2011) 656 završno, Bruxelles, 20. listopada 2011.; Europska komisija (2011), *Prijedlog uredbe Europskog parlamenta i Vijeća o tržištima financijskih instrumenata i izmjeni Uredbe [EMIR] o OTC izvedenicama, središnjoj drugoj ugovornoj strani i trgovinskom repozitoriju*, COM(2011) 652 završno, Bruxelles, 20. listopada 2011.; Europska komisija (2011), *Prijedlog Direktive Europskog parlamenta i Vijeća o pristupu aktivnosti kreditnih institucija i bonitetnom nadzoru kreditnih institucija i investicijskih društava i o izmjeni Direktive 2002/87/EZ Europskog parlamenta i Vijeća o dodatnom nadzoru kreditnih institucija, društava za osiguranje i investicijskih društava u financijskom konglomeratu*, COM(2011) 453 završno, Bruxelles, 20. srpnja 2011.

320 Europska komisija (2011), *Prijedlog uredbe Europskog parlamenta i Vijeća o trgovanju na temelju povlaštenih informacija i manipuliranju tržištem (zlouporabi tržišta)*, COM(2011) 651 završno, Bruxelles, 20. listopada 2011.; Europska komisija (2011), *Prijedlog direktive Europskog parlamenta i Vijeća o kaznenim sankcijama za trgovanje na temelju povlaštenih informacija i manipuliranje tržištem*, COM(2011) 654 završno, Bruxelles, 20. listopada 2011.

- otkrivanje osobnih informacija, uključujući objavu sankcija
- ovlaštenje nadležnih tijela da provode nadzor i istrage, uključujući terenske preglede i ulazak u privatne prostorije radi oduzimanja dokumenata
- mehanizmi za prijavu kršenja, npr. program dojava
- suradnja između nadležnih tijeka država članica i Europskog nadzornog tijela za vrijednosne papire i tržišta kapitala (ESMA).

I druga su pitanja u tim područjima posebno obrađena, uključujući prikupljanje podataka o financijskom statusu osobe čiji se podaci obrađuju[321] ili prekograničnim plaćanjima putem bankovnih prijenosa, što neizbježno dovodi do prijenosa osobnih podataka.[322]

321 Uredba (EZ) br. 1060/2009 Europskog parlamenta i Vijeća od 16 rujna 2009. o agencijama za kreditni rejting, SL 2009 L 302; Europska komisija, *Prijedlog uredbe Europskog parlamenta i Vijeća o izmjeni Uredbe (EZ) br. 1060/2009 o agencijama za kreditni rejting*, COM(2010) 289 završno, Bruxelles, 2. lipnja 2010.

322 Direktiva 2007/64/EZ Europskog parlamenta i Vijeća od 13. studenoga 2007. o uslugama platnog prometa na unutarnjem tržištu i o izmjeni direktiva 97/7/EZ, 2002/65/EZ, 2005/60/EZ i 2006/48/EZ te stavljanju izvan snage Direktive 97/5/EZ, SL 2007 L 319.

Dodatna literatura

Prvo poglavlje

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*, Vienna, Manzsche Verlags- und Universitätsbuchhandlung.

EDRi, *An introduction to data protection*, Bruxelles, www.edri.org/files/paper06_datap.pdf.

Frowein, J. i Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

Grabenwarter, C. i Pabel, K. (2012), *Europäische Menschenrechtskonvention*, München, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. i Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union,* München, C. H. Beck.

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*, Antwerp, 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., www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

White, R. i Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Drugo poglavlje

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

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.

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.

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*, www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation.

Od trećeg do petog poglavlja

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.

Dammann, U. i Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

FRA (Agencija Europske unije za temeljna prava) (2010), *Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II)*, Luksemburg, Ured za publikacije Europske unije (Ured 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, Ured za publikacije.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*, www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.

Šesto poglavlje

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.

Sedmo poglavlje

Europol (2012), *Data Protection at Europol*, Luksemburg, Ured za publikacije, www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, Haag, Eurojust.

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.

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*, Centar za pravo vanjskih odnosa, CLEER radni dokumenti 2013/2, www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

Osmo poglavlje

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.

Sudska praksa

Odabrana sudska praksa Europskog suda za ljudska prava

Pristup osobnim podacima

Gaskin protiv Ujedinjene Kraljevine, br. 10454/83, 7. srpnja 1989.
Godelli protiv Italije, br. 33783/09, 25. rujna 2012.
K.H. i drugi protiv Slovačke, br. 32881/04, 28. travnja 2009.
Leander protiv Švedske, br. 9248/81, 26. ožujka 1987.
Odièvre protiv Francuske [GC], br. 42326/98, 13. veljače 2003.

Uravnoteživanje zaštite podataka i slobode izražavanja

Axel Springer AG protiv Njemačke [GC], br. 39954/08, 7. veljače 2012.
Von Hannover protiv Njemačke, br. 59320/00, 24. lipnja 2004.
Von Hannover protiv Njemačke (br. 2) [GC], br. 40660/08 i 60641/08, 7. veljače 2012.

Izazovi elektroničke zaštite podataka

K.U. protiv Finske, br. 2872/02, 2. prosinca 2008.

Dopisivanje

Amann protiv Švicarske [GC], br. 27798/95, 16. veljače 2000.
Bernh Larsen Holding AS i drugi protiv Norveške, br. 24117/08, 14. ožujka 2013.

Cemalettin Canli protiv Turske, br. 22427/04, 18. studenoga 2008.
Dalea protiv Francuske, br. 964/07, 2. veljače 2010.
Gaskin protiv Ujedinjene Kraljevine, br. 10454/83, 7. srpnja 1989.
Haralambie protiv Rumunjske, br. 21737/03, 27. listopada 2009.
Khelili protiv Švicarske, br. 16188/07, 18. listopada 2011.
Leander protiv Švedske, br. 9248/81, 26. ožujka 1987.
Malone protiv Ujedinjene Kraljevine, br. 8691/79, 26. travnja 1985.
McMichael protiv Ujedinjene Kraljevine, br. 16424/90, 24. veljače 1995.
M.G. protiv Ujedinjene Kraljevine, br. 39393/98, 24. rujna 2002.
Rotaru protiv Rumunjske [GC], br. 28341/95, 4. svibnja 2000.
S. i Marper protiv Ujedinjene Kraljevine, br. 30562/04 i 30566/04, 4. prosinca 2008.
Shimovolos protiv Rusije, br. 30194/09, 21. lipnja 2011.
Turek protiv Slovačke, br. 57986/00, 14. veljače 2006.

Baze podataka o kaznenim evidencijama

B.B. protiv Francuske, br. 5335/06, 17. prosinca 2009.
M.M. protiv Ujedinjene Kraljevine, br. 24029/07, 13. studenoga 2012.

Baze podataka o DNK

S. i Marper protiv Ujedinjene Kraljevine, br. 30562/04 i 30566/04, 4. prosinca 2008.

Podaci GPS-a

Uzun protiv Njemačke, br. 35623/05, 2. rujna 2010.

Zdravstveni podaci

Biriuk protiv Litve, br. 23373/03, 25. studenog 2008.
I. protiv Finske, br. 20511/03, 17. srpnja 2008.
L.L. protiv Francuske, br. 7508/02, 10. listopada 2006.
M.S. protiv Švedske, br. 34209/96, 2. srpnja 2002.
Szuluk protiv Ujedinjene Kraljevine, br. 36936/05, 2. lipnja 2009.
Z. protiv Finske, br. 22009/93, 25. veljače 1997.

Identitet

Ciubotaru protiv Moldavije, br. 27138/04, 27. travnja 2010.
Godelli protiv Italije, br. 33783/09, 25. rujna 2012.
Odièvre protiv Francuske [GC], br. 42326/98, 13. veljače 2003.

Informacije u vezi s profesionalnim aktivnostima

Michaud protiv Francuske, br. 12323/11, 6. prosinca 2012.
Niemietz protiv Njemačke, br. 13710/88, 16. prosinca 1992.

Presretanje komunikacije

Amann protiv Švicarske [GC], br. 27798/95, 16. veljače 2000.
Copland protiv Ujedinjene Kraljevine, br. 62617/00, 3. travnja 2007.
Cotlet protiv Rumunjske, br. 38565/97, 3. lipnja 2003.
Kruslin protiv Francuske, br. 11801/85, 24. travnja 1990.
Lambert protiv Francuske, br. 23618/94, 24. kolovoza 1998.
Liberty i drugi protiv Ujedinjene Kraljevine, br. 58243/00, 1. srpnja 2008.
Malone protiv Ujedinjene Kraljevine, br. 8691/79, 26. travnja 1985.
Halford protiv Ujedinjene Kraljevine, br. 20605/92, 25. lipnja 1997.
Szuluk protiv Ujedinjene Kraljevine, br. 36936/05, 2. lipnja 2009.

Obveze nositelja dužnosti

B.B. protiv Francuske, br. 5335/06, 17. prosinca 2009.
I. protiv Finske, br. 20511/03, 17. srpnja 2008.
Mosley protiv Ujedinjene Kraljevine, br. 48009/08, 10. svibnja 2011.

Fotografije

Sciacca protiv Italije, br. 50774/99, 11. siječnja 2005.
Von Hannover protiv Njemačke, br. 59320/00, 24. lipnja 2004.

Pravo na zaborav

Segerstedt-Wiberg i drugi protiv Švedske, br. 62332/00, 6. lipnja 2006.

Pravo na prigovor

Leander protiv Švedske, br. 9248/81, 26. ožujka 1987.
Mosley protiv Ujedinjene Kraljevine, br. 48009/08, 10. svibnja 2011.
M.S. protiv Švedske, br. 34209/96, 2. srpnja 2002.
Rotaru protiv Rumunjske [GC], br. 28341/95, 4. svibnja 2000.

Osjetljive kategorije podataka

I. protiv Finske, br. 20511/03, 17. srpnja 2008.

Michaud protiv Francuske, br. 12323/11, 6. prosinca 2012.
S. i Marper protiv Ujedinjene Kraljevine, br. 30562/04 i 30566/04, 4. prosinca 2008.

Nadzor i provedba (uloga raznih subjekata, uključujući tijela za zaštitu podataka)

I. protiv Finske, br. 20511/03, 17. srpnja 2008.
K.U. protiv Finske, br. 2872/02, 2. prosinca 2008.
Von Hannover protiv Njemačke, br. 59320/00, 24. lipnja 2004.
Von Hannover protiv Njemačke (br. 2) [GC], br. 40660/08 i 60641/08, 7. veljače 2012.

Metode nadzora

Allan protiv Ujedinjene Kraljevine, br. 48539/99, 5. studenoga 2002.
Udruga „21 Décembre 1989" i drugi protiv Rumunjske, br. 33810/07 i 18817/08, 24. svibnja 2011.
Bykov protiv Rusije [GC], br. 4378/02, 10. ožujka 2009.
Kennedy protiv Ujedinjene Kraljevine, br. 26839/05, 18. svibnja 2010.
Klass i drugi protiv Njemačke, br. 5029/71, 6. rujna 1978.
Rotaru protiv Rumunjske [GC], br. 28341/95, 4. svibnja 2000.
Taylor-Sabori protiv Ujedinjene Kraljevine, br. 47114/99, 22. listopada 2003.
Uzun protiv Njemačke, br. 35623/05, 2. rujna 2010.
Vetter protiv Francuske, br. 59842/00, 31. svibnja 2005.

Videonadzor

Köpke protiv Njemačke, br. 420/07, 5. listopada 2010.
Peck protiv Ujedinjene Kraljevine, br. 44647/98, 28. siječnja 2003.

Glasovni uzorci

P.G. i J.H. protiv Ujedinjene Kraljevine, br. 44787/98, 25. rujna 2001.
Wisse protiv Francuske, br. 71611/01, 20. prosinca 2005.

Odabrana sudska praksa Suda Europske unije

Sudska praksa vezana uz Direktivu o zaštiti podataka

Zajednički slučajevi C-293/12 i C-594/12, *Digital Rights Ireland i Seitling i drugi*, 8. travnja 2014.
[Kršenje primarnog prava Europske unije Direktivom o zadržavanju podataka]

C-73/07, *Tietosuojavaltuutettu protiv Satakunnan Markkinapörssi Oy i Satamedia Oy*, 16. prosinca 2008.
[pojam „novinarskih djelatnosti" u smislu članka 9. Direktive o zaštiti podataka]

Zajednički slučajevi C-92/09 i C-93/09, *Volker i Markus Schecke GbR i Hartmut Eifert protiv Land Hessen*, 9. studenoga 2010.
[Razmjernost pravne obveze objavljivanja osobnih podataka o korisnicima određenih potpora iz poljoprivrednih fondova Europske unije]

C-101/01, *Bodil Lindqvist*, 6. studenoga 2003.
[Zakonitost internetske objave podataka o privatnom životu drugih od strane fizičke osobe]

C-131/12, *Google Spain, S.L., Google Inc. protiv Agencia Española de Protección de Datos, Mario Costeja González*, Zahtjev za prethodnom odlukom suda *Audiencia Nacional* (Španjolska) podnesen 9. ožujka 2012., 25. svibnja 2012., u tijeku
[Obveze suzdržavanja pružatelja usluga internetskih pretraživača od prikazivanja osobnih podataka u rezultatima pretraživanja na zahtjev osobe čiji se podaci obrađuju]

C-270/11, *Europska komisija protiv Kraljevine Švedske*, 30. svibnja 2013.
[Kazna za neprovođenje direktive]

C-275/06, *Productores de Música de España (Promusicae) protiv Telefónica de España SAU*, 29. siječnja 2008.
[Obveze pružatelja usluga internetskog pristupa vezane uz otkrivanje identiteta korisnika programa razmjene datoteka KaZaA udruzi za zaštitu intelektualnog vlasništva]

C-288/12, *Europska komisija protiv Mađarske*, tužba podnesena 8. travnja 2012.
[Zakonitost ukidanja službe nacionalnog nadzornika za zaštitu podataka]

C-291/12, *Michael Schwarz protiv Stadt Bochum*, mišljenje neovisnog odvjetnika, 13. lipnja 2013.
[Kršenje primarnog prava Europske unije Uredbom (EZ) 2252/2004 o obvezi uvođenja otisaka prstiju u putovnicama]

C-360/10, *SABAM protiv Netlog N.V.*, 16. veljače 2012.
[Obveza pružatelja usluga društvenih mreža vezana uz sprečavanje nezakonite uporabe glazbenih i audio-vizualnih uradaka od strane internetskih korisnika]

Zajednički slučajevi C-465/00, C-138/01 i C-139/01, *Rechnungshof protiv Österreichischer Rundfunk i drugih i Neukomm i Lauermann protiv Österreichischer Rundfunk*, 20. svibnja 2003.
[Razmjernost pravne obveze objave osobnih podataka o plaćama zaposlenika određenih kategorija institucija povezanih s javnim sektorom]

Zajednički slučajevi 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. studenoga 2011.
[Točna provedba članka 7. točke (f) Direktive o zaštiti privatnosti – „zakoniti interesi drugih" – u nacionalnom zakonodavstvu]

C-518/07, *Europska komisija protiv Savezne Republike Njemačke*, 9. ožujka 2010.
[Neovisnost nacionalnog nadzornog tijela]

C-524/06, *Huber protiv Bundesrepublik Deutschland*, 16. prosinca 2008.
[Zakonitost zadržavanja podataka o strancima u statističkom registru]

C-543/09, *Deutsche Telekom AG protiv Bundesrepublik Deutschland*, 5. svibnja 2011.
[Nužnost obnavljanja suglasnosti]

C-553/07, *College van burgemeester en wethouders van Rotterdam protiv M.E.E. Rijkeboer*, 7. svibnja 2009.
[Pravo pristupa osobe čiji se podaci obrađuju]

C-614/10, *Europska komisija protiv Republike Austrije*, 16. listopada 2012.
[Neovisnost nacionalnog nadzornog tijela]

Sudska praksa vezana uz Uredbu o zaštiti podataka u institucijama Europske unije

C-28/08 P, *Europska komisija protiv The Bavarian Lager Co. Ltd*, 29. lipnja 2010.
[Pristup dokumentima]

C-41/00 P, *Interporc Im- und Export GmbH protiv Komisije Europskih zajednica*, 6. ožujka 2003.
[Pristup dokumentima]

F-35/08, *Pachtitis protiv Komisije i EPSO-a*, 15. lipnja 2010.
[Uporaba osobnih podataka u kontekstu zapošljavanja u institucijama Europske unije]

F-46/09 *V protiv Parlamenta*, 5. srpnja 2011.
[Uporaba osobnih podataka u kontekstu zapošljavanja u institucijama Europske unije]

Popis predmeta

Sudska praksa Europskog suda pravde

Sudska praksa Europskog suda za ljudska prava

Sudska praksa nacionalnih sudova

Agencija Europske unije za temeljna prava
Europski sud za ljudska prava – Vijeće Europe

Priručnik o europskom zakonodavstvu o zaštiti podataka

2014 — 195 str. — 14,8 × 21 cm

ISBN 978-92-871-9945-4 (CoE)
ISBN 978-92-9239-333-5 (FRA)
doi:10.2811/53863

Daljnje informacije o Agenciji Europske unije za temeljna prava dostupne su na internetu putem FRA web stranice (fra.europa.eu).

Dodatne informacije o Vijeću Europe dostupne su na internetu, putem web stranice: hub.coe.int.

Dodatne informacije o sudskoj praksi Europskog suda za ljudska prava dostupne su na web stranici Suda: echr.coe.int. Internetski portal HUDOC omogućuje pretraživanje presuda i odluka na engleskom i / ili francuskom jeziku, pristup prijevodima na druge jezike, kao i mjesečnim bilješkama o sudskoj praksi, priopćenjima za tisak i drugim informacijama o radu Suda.

10.2811/53863
TK-01-13-772-HR-C

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

Sve brži razvoj informacijskih i komunikacijskih tehnologija za sobom povlači i rastuću potrebu za snažnom zaštitom osobnih podataka. To je pravo zaštićeno i instrumentima Europske unije (EU) i instrumentima Vijeća Europe (CoE). Tehnološka dostignuća šire granice primjerice nadzora, presretanja komunikacije i pohrane podataka pa je sve izazovnija zadaća očuvati pravo na zaštitu podataka. Cilj je ovoga priručnika upoznati pravnike koji nisu specijalizirani u području zaštite podataka s tom pravnom granom. Priručnik sadrži pregled primjenjivih pravnih okvira Europske unije i Vijeća Europe. Sažimajući glavne presude Europskog suda za ljudska prava (ECtHR) i Suda Europske unije (CJEU), donosi objašnjenja vezana uz ključnu sudsku praksu. U slučaju da nije zabilježena sudska praksa, daje praktične ilustracije s hipotetskim scenarijima. Priručnikom se ukratko želi doprinijeti odlučnoj i snažnoj provedbi prava na zaštitu podataka.

AGENCIJA EUROPSKE UNIJE ZA TEMELJNA PRAVA
Schwarzenbergplatz 11 – 1040 Beč – Austria
Tel. +43 (1) 580 30-60 – Faks +43 (1) 580 30-693
fra.europa.eu – info@fra.europa.eu

VIJEĆE EUROPE
EUROPSKI SUD ZA LJUDSKA PRAVA
67075 Strasbourg Cedex – Francuska
Tel. +33 (0) 3 88 41 20 00 – Faks +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int

Ured za publikacije

ISBN 978-92-871-9945-4 (CoE)
ISBN 978-92-9239-333-5 (FRA)