Partnership for Good Governance

Parteneriat pentru o bună guvernare
Consolidarea dreptului la protecția datelor în țările Parteneriatului estic

Manual de formare cu privire la rolul și misiunile autorităților de protecție a datelor

REZUMAT

Scopul prezentului manual de formare este de a oferi o descriere generală a rolului și misiunii autorităților de protecție a datelor, punându-se un accent deosebit pe experiențele țărilor vizate de Parteneriatul pentru o bună guvernare (PGG), și anume Armenia, Azerbaidjan, Georgia, Moldova, Ucraina și Belarus.

Acesta este prevăzut a ajuta autoritățile de protecție a datelor nou înființate sau membrii noi ai acestor autorități să înțeleagă mai bine particularitățile și specificul autorităților de protecție a datelor.

Se pune un accent deosebit pe provocările care apar la instituirea autorității (motivele înființării unei autorități de protecție a datelor, cerințele privind independența, definirea unei strategii și a unui program de lucru, definirea unei structuri și a unei organigrame etc.).

Apoi, este descris cu atenție rolul consultativ al autorității de protecție a datelor. Acest rol devine din ce în ce mai diversificat, iar autoritatea de protecție a datelor ar putea fi implicată cu privire la mai multe aspecte: proceduri de notificare și de autorizare; avize cu privire la proiecte de legi; definirea de modele și orientări la nivel sectorial; elaborarea de instrumente de responsabilizare; stabilirea de relații cu cercuri de cercetare și inovare etc.

Apoi, acest manual de formare abordează competențele de supraveghere ale unei autorități de protecție a datelor. Acesta descrie competențele *ex post* ale autorității: soluționarea plângerilor persoanelor; verificările operatorilor; adoptarea sancțiunilor; capacitatea de a aduce un caz în atenția autorităților judiciare etc.

De asemenea, este abordată nevoia de a institui o strategie de comunicare și de a derula campanii de sensibilizare.

În final, sunt descrise activitățile de cooperare și cele internaționale ale autorităților.

CUPRINS

INTRODUCERE

Evoluția rapidă și constantă a tehnologiilor informației și comunicațiilor este extrem de benefică pentru persoane și ar trebui să fie încurajată. În același timp, persoanele se pot confrunta și cu provocările pe care le prezintă un flux continuu de date, care ar putea lua diverse forme: volume mari de date, internetul obiectelor, tehnologia de tip cloud computing, supravegherea în masă, supravegherea video, crearea de profiluri, evaluarea bonității, publicitatea comportamentală, marketing direct, geolocalizarea prin cipuri RFID sau
conexiuni Wi-Fi, identificarea biometrică etc.

Această revoluție tehnologică aduce problema confidențialității și a protecției datelor cu caracter personal în centrul sistemului nostru social și politic.

Autoritățile de protecție a datelor, având rolul, misiunile și competențele descrise în prezentul manual, joacă un rol din ce în ce mai strategic pentru protejarea drepturilor și libertăților fundamentale ale persoanelor în era digitală.

1. Protecția dreptului la confidențialitate la nivel internațional

1. Organizația Națiunilor Unite

Articolul 12 din Declarația universală a drepturilor omului, proclamată de către Adunarea Generală a **ONU** la Paris la 10 decembrie 1948 (Rezoluția 217 A), prevede că „Nimeni nu va fi supus la imixtiuni arbitrare în viața sa personală, în familia sa, în domiciliul lui sau în corespondența sa, nici la atingeri aduse onoarei și reputației sale. Orice persoană are dreptul la protecția legii împotriva unor asemenea imixtiuni sau atingeri*”*.

Această declarație constituie un document de referință în istoria drepturilor omului și a fost tradusă în peste 500 de limbi. La baza vieții private se află demnitatea umană și alte valori-cheie, precum libertatea de asociere și libertatea de exprimare. Aceasta a devenit una dintre problemele fundamentale în materie de drepturi ale omului în epoca modernă.

Articolul 17 din Pactul internațional cu privire la drepturile civile și politice, care a fost adoptat prin Rezoluția 2200A (XXI) a Adunării Generale a Organizației Națiunilor Unite (XXI) din 16 decembrie 1966, protejează, de asemenea, dreptul la viața privată.

Articolul 16 din Convenția privind drepturile copilului, adoptată prin Rezoluția 44/25 din 20 noiembrie 1989 a Adunării Generale, prevede că „Nici un copil nu va fi supus unei imixtiuni arbitrare sau ilegale în viața sa privată, în familia sa, în domiciliul său ori în corespondența sa, precum și nici unui fel de atac ilegal la onoarea și reputația sa”.

Alte instrumente internaționale privind drepturile omului conțin dispoziții similare. Deși dreptul la viața privată prevăzut prin legislația internațională în materie de drepturi ale omului nu este absolut, orice ingerință trebuie să fie prevăzută prin lege și supusă unei analize atente și critice a necesității, caracterului legitim și proporționalității acesteia în raport cu scopul legitim urmărit.

2. Consiliul Europei

La nivelul **Consiliului Europei**, articolul 8 din Convenția europeană a drepturilor omului (CEDO) prevede că „Orice persoană are dreptul la **respectarea vieții sale private și de familie**, a domiciliului său și a corespondenței sale.”

În conformitate cu jurisprudența extinsă a Curții Europene a Drepturilor Omului[1], dreptul la viața privată semnifică importanța demnității personale și a autonomiei, precum și interacțiunea unei persoane cu altele, atât la nivel personal, cât și public. Acesta cuprinde dreptul de a stabili și a dezvolta relații cu alte ființe umane, în special la nivel emoțional, pentru dezvoltarea și formarea propriei personalități.

Respectarea vieții private a unei persoane include, spre exemplu, și respectarea dreptului la imagine, a dreptului la autonomia personală, respectarea vieții sexuale, respectarea informațiilor personale și confidențiale, a dreptului de a nu fi supus supravegherii ilegale din partea statului, a dreptului de a controla informațiile despre viața privată a unei persoane etc.

2. Evoluția istorică a unui anumit drept la protecția datelor cu caracter personal la nivel național

La începutul anilor 1970, mai multe țări au început să adopte legi cu caracter general prevăzute pentru a proteja viața privată a persoanelor odată cu evoluția tehnologiei informației. Potențialul de supraveghere al tehnologiilor informațiilor a dus la dezvoltarea unor reguli specifice care reglementează colectarea și manipularea datelor cu caracter personal pentru a preveni abuzurile.

Începuturile legislației în acest domeniu pot fi regăsite în primele acte legislative privind protecția datelor adoptate în landul Hessen din Germania în 1970. Acestea au fost urmate de legi naționale adoptate în Suedia (1973), Statele Unite (în 1974, o lege doar pentru agenții federale) sau în Germania (1977), Franța și Luxemburg (1978).

Protecția datelor a fost integrată, de asemenea, ca un drept fundamental în mai multe constituții (în special articolul 35 din Constituția Portugaliei din 1976; articolul 18 din Constituția Spaniei din 1978).

Spre exemplu, în Franța, guvernul francez a anunțat în 1974 un plan cunoscut drept SAFARI („Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus”), conceput pentru a identifica fiecare cetățean cu un anumit număr și, pe baza acelui identificator unic, pentru a interconecta toate evidențele statului.

Acest plan a generat mari controverse în rândul opiniei publice după publicarea unui articol în jurnalul „Le Monde” la 24 martie 1974. Acesta a subliniat pericolele inerente anumitor utilizări ale tehnologiei informației și a exprimat unele temeri cu privire la faptul că întreaga populație franceză va fi înregistrată în curând în dosare fără niciun control democratic corespunzător. Această teamă a determinat guvernul să înființeze o comisie însărcinată cu recomandarea de

[1] http://www.echr.coe.int/Pages/home.aspx?p=home&c=fre

măsuri concrete menite să garanteze faptul că orice evoluții ale tehnologiei informației vor asigura în continuare respectarea vieții private, a drepturilor personale și a libertăților publice.

După ample dezbateri și consultări publice, s-a stabilit să se înființeze o autoritate de supraveghere administrativă independentă, denumită „Comisia pentru Tehnologia Informației și a Libertăților" (Commission Nationale de l'Informatique et des Libertés sau CNIL), pentru a monitoriza punerea în aplicare a legii franceze în materie de protecție a persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, adoptată la data de 6 ianuarie 1978[2].

Un număr mare de țări din lume, de pe toate continentele, au adoptat legislații privind protecția datelor. În 2017, 115 de autorități de protecție a datelor sunt membri ai Conferinței Internaționale a Comisarilor pentru Protecția Datelor și a Vieții Private[3].

3. Evoluția dreptului la protecția datelor cu caracter personal la nivel european și internațional

1. Consiliul Europei

Creșterea rapidă a fluxurilor de date cu caracter personal între organizații și la nivel transfrontalier a generat noi riscuri pentru protecția sferei private a persoanelor la nivel internațional. În același timp, legislațiile naționale în domeniul protecției persoanelor cu privire la prelucrarea datelor cu caracter personal au fost, în majoritatea cazurilor, inexistente. Totuși, nu a fost elaborat un model uniform de protecție.

Având în vedere această tendință, reprezentanții guvernelor din cadrul **Consiliului Europei** au decis să stabilească un cadru de principii și norme specifice pentru a preveni colectarea și prelucrarea inechitabilă a datelor cu caracter personal[4].

Un prim pas în această direcție a fost făcut în 1973 și 1974, odată cu adoptarea Rezoluțiilor (73) 22 și (74) 29 care au stabilit principii pentru protecția datelor cu caracter personal din băncile de date automatizate în sectorul privat și public.

În final, Convenția pentru „protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal" („**Convenția 108**") a Consiliului Europei a fost deschisă pentru semnare la 28 ianuarie 1981 după patru ani de negocieri. Este primul instrument internațional cu caracter obligatoriu care protejează persoanele de abuzuri care pot decurge din prelucrarea datelor cu caracter personal și care caută să asigure cadrul pentru fluxurile internaționale de date cu caracter personal.

Aceste **principii** prevăzute în Convenția 108 se referă, în mod special, la prelucrarea automată echitabilă și legală a datelor în scopuri legitime specifice. Acestea vizează, de asemenea, calitatea datelor, care trebuie să fie adecvate, relevante și neexcesive. Mai mult, persoanele sunt pe deplin

[2] https://www.cnil.fr/en/cnils-facts-and-numbers
[3] https://icdppc.org/the-conference-and-executive-committee/history-of-the-conference/
[4] http://www.coe.int/en/web/data-protection/background

informate cu privire la prelucrarea datelor lor cu caracter personal și trebuie să aibă dreptul de a le accesa, a le rectifica și a le șterge.

În plus față de faptul că oferă garanții în legătură cu prelucrarea datelor cu caracter personal, aceasta scoate în afara legii prelucrarea **datelor „cu caracter sensibil”** (date legate de rasa, convingerile politice, sănătatea, religia, viața sexuală, cazierul etc. al persoanei) în absența unor garanții legale.

Convenția prevede libera circulație a datelor cu caracter personal între statele părți la Convenție, cu excepția cazului în care protecția datelor cu caracter personal din celălalt stat parte nu este „echivalentă” sau dacă datele sunt transferate într-un stat terț care nu este parte la Convenție.

Convenția prevede înființarea unui **comitet consultativ**, care este format din reprezentanți ai părților la Convenție, fiind completat de observatori din alte state (membre sau nemembre) și actori nestatali, organizații internaționale etc.

În anul 2001 a fost deschis, pentru semnare, un protocol adițional la Convenția 108 cu privire la autoritățile de supraveghere și fluxurile de date transfrontaliere, reafirmând misiunea și competențele autorităților de supraveghere și interzicând transferul datelor cu caracter personal în state sau către organizații care nu asigură un nivel adecvat de protecție.

În noiembrie 2017, 51 de state sunt părți la Convenția 108, inclusiv țări care nu sunt membre ale Consiliului Europei, precum Mauritius, Senegal, Tunisia sau Uruguay[5] (alte țări precum Burkina Faso, Maroc, Republica Capul Verde și Argentina fiind invitate să adere), consolidând potențialul Convenției 108 de a constitui un standard global de norme privind protecția datelor.

În 2010, pe de o parte pentru a aborda mai bine provocările asociate utilizării de tehnologii noi ale informației și comunicațiilor și, pe de altă parte, pentru a consolida punerea în aplicare a Convenției 108, **a fost activat procesul de modernizare a Convenției 108**, acesta fiind în prezent în ultima etapă.

De asemenea, ar trebui menționat **rolul din ce în ce mai important al jurisprudenței Curții Europene a Drepturilor Omului** în domeniul protecției datelor cu caracter personal. Curtea reamintește că „protecția datelor cu caracter personal (...) este extrem de importantă pentru exercitarea dreptului persoanelor la respectarea vieții lor private și de familie, astfel cum este garantat prin articolul 8 din Convenție” (a se consulta CtEDO, M.S. c. *Suediei*, 27 august 1997, n°74/1996/693/885).

Cu privire la protecția datelor cu caracter personal, Curtea Europeană a Drepturilor Omului a elaborat o jurisprudență vastă[6].

[5] http://www.coe.int/en/web/data-protection/parties

[6] A se consulta Handbook on European data protection law (Manual privind dreptul european în materie de protecție a datelor), publicat de către Consiliul Europei și Agenția UE pentru Drepturi Fundamentale (EU Fundamental Rights Agency): https://rm.coe.int/16806b294a; A se consulta, de asemenea, Fișa informativă a Curții Europene a Drepturilor Omului privind protecția datelor cu caracter personal: http://www.echr.coe.int/Documents/FS_Data_ENG.pdf

2. OCDE

La nivelul **Organizației pentru Cooperare și Dezvoltare Economică (OCDE)**, au fost adoptate mai multe inițiative pe la sfârșitul anilor 1970. Țările membre ale OCDE au considerat că este necesar să se elaboreze orientări care să ajute la armonizarea legislațiilor naționale în materie de confidențialitate și să se prevină totodată întreruperile de fluxuri de date la nivel internațional.

Orientările, care iau forma unei recomandări a Consiliului OCDE, au fost elaborate de către un grup de experți guvernamentali. Recomandarea a fost adoptată și a devenit aplicabilă la 23 septembrie 1980.

Principiile de bază ale aplicării la nivel național, care sunt cuprinse în orientări, sunt următoarele, acestea fiind foarte apropiate de cele prevăzute în Convenția 108: principiul limitării colectării; principiul calității datelor, principiul specificării scopului, principiul limitării utilizării, principiul garanțiilor de securitate, principiul deschiderii, principiul participării individuale (dreptul de acces etc.), principiul răspunderii[7].

Prezentele orientări au fost actualizate în anul 2013. Există două tematici abordate în orientările actualizate:

- obiectivul punerii în aplicare a protecției vieții private printr-o abordare ancorată în gestionarea riscurilor, și;
- nevoia de a aborda dimensiunea globală a vieții private printr-o interoperabilitate îmbunătățită[8].

3. Organizația Națiunilor Unite

La nivelul Organizației Națiunilor Unite, ar putea fi menționate principiile directoare de reglementare a fișierelor electronice care conțin date cu caracter personal, adoptate în mod unanim prin Rezoluția Adunării Generale 45/95 din 14 decembrie 1990.

Principiile directoare prevăd zece principii care oferă garanții minime de protecție a datelor cu caracter personal în ceea ce privește viața privată: legalitate și echitabilitate; exactitate; indicarea scopului; accesul persoanei interesate; nediscriminare; competența de a face excepții, în anumite cazuri, de la primele cinci principii; principiul securității; supravegherea de către o autoritate și aplicarea de sancțiuni; libera circulație a datelor între țări atunci când acestea au asigurat „garanții comparabile pentru protecția vieții private"; aplicabilitatea principiilor în cazul „tuturor fișierelor computerizate publice și private"[9].

În aprilie 2015, ca urmare a afirmațiilor revelatoare ale lui Edward Snowden cu privire la supravegherea masivă și o rezoluție a Adunării Generale în acest sens, Consiliul ONU pentru Drepturile Omului a adoptat Rezoluția 28/16 care decide să numească, pentru prima dată și pentru o perioadă de trei ani, un raportor special cu privire la dreptul la viața privată[10].

[7] http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
[8] http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm
[9] http://www.un.org/documents/ga/res/45/a45r095.htm
[10] Cf. http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx

4. Uniunea Europeană

În cadrul **Uniunii Europene**, articolele 7 și 8 din Carta Drepturilor Fundamentale prevede faptul că fiecare persoană are dreptul la respectarea vieții sale private și de familie, a domiciliului și a comunicațiilor și că fiecare are dreptul la protecția datelor sale cu caracter personal.
Înaintea adoptării Cartei, în anul 1995, cunoscând deficiențele legilor și numeroasele diferențe de la nivelul protecției în fiecare dintre statele sale membre, Uniunea Europeană a adoptat o directivă la nivelul Europei.

Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 a fost prevăzută pentru a oferi un cadru de reglementare pentru a garanta circulația sigură și liberă a datelor cu caracter personal peste granițele naționale ale statelor membre ale UE[11].

Operatorii trebuie să respecte drepturile privind viața privată și protecția datelor ale persoanelor ale căror date cu caracter personal le sunt încredințate. Acestea trebuie, spre exemplu:

- să colecteze și să prelucreze date cu caracter personal în mod echitabil și deschis, pentru un scop legitim, în mod proporțional și cu precizie și să asigure actualizarea datelor; etc.;
- să asigure existența unui temei legitim pentru prelucrarea datelor cu caracter personal;
- să se abțină, cu anumite excepții, de la a colecta categorii speciale de date care sunt considerate drept date cu caracter sensibil;
- să se asigure de securitatea datelor cu caracter personal;
- să informeze persoanele în legătură cu prelucrarea și să asigure dreptul de acces la date sau dreptul de a contesta prelucrarea datelor;
- să respecte anumite obligații cu privire la prelucrarea datelor cu caracter personal;
- să răspundă la plângerile cu privire la încălcările normelor privind protecția datelor;
- să colaboreze cu autoritățile naționale de supraveghere a protecției datelor; etc.

Această directivă privind protecția datelor a fost completată de alte instrumente juridice.

Ar putea fi menționată, în special, Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice), cunoscută drept Directiva privind confidențialitatea electronică[12]. Această directivă cuprinde, în mod specific, anumite cerințe privind confidențialitatea comunicațiilor electronice, securitatea rețelelor și a serviciilor, notificări privind încălcarea datelor, date despre trafic și locații, mesaje de tip spam, directoare publice sau identificarea liniei de apelare[13].

Există, de asemenea, norme specifice pentru protecția datelor cu caracter personal în cooperarea polițienească și judiciară în materie penală adoptată prin Decizia-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008[14]. Protecția datelor cu caracter personal colectate de către instituțiile și organismele Uniunii Europene este asigurată prin Regulamentul nr. 45/2001[15].

[11] http://eur-lex.europa.eu/legal-content/EN-RO/TXT/?uri=CELEX:31995L0046&fromTab=ALL&from=en
[12] http://eur-lex.europa.eu/legal-content/EN-RO/TXT/?uri=CELEX:32002L0058&fromTab=ALL&from=RO
[13] https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive
[14] http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32008F0977
[15] http://ec.europa.eu/justice/policies/privacy/docs/application/286_en.pdf

5. Regulamentul general privind protecția datelor sau „RGPD”

În ianuarie 2012, Comisia Europeană a propus **o reformă complexă a normelor privind protecția datelor în UE.** La data de 4 mai 2016, în urma mai multor ani de negocieri, textele oficiale ale noului Regulament și ale noii Directive au fost publicate în Jurnalul Oficial al Uniunii Europene în toate limbile oficiale.

Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (**Regulamentul general privind protecția datelor sau „RGPD”)** va deveni complet aplicabil începând cu 25 mai 2018[16].

Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date, a intrat în vigoare la data de 5 mai 2016, iar statele membre UE au obligația de a o transpune în legislația națională până la 6 mai 2018[17].

Obiectivul acestui nou set de norme este să redea persoanelor fizice controlul asupra propriilor date cu caracter personal, să simplifice cadrul normativ pentru companii și să armonizeze legislațiile privind protecția datelor în rândul tuturor țărilor europene.

Directiva privind confidențialitatea electronică și Regulamentul nr. 45/2001 sunt, de asemenea, în curs de revizuire.

[16] http://eur-lex.europa.eu/legal-content/ro/TXT/?uri=CELEX%3A32016R0679
[17] http://eur-lex.europa.eu/legal-c
content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC

4. Consolidarea dreptului la protecția datelor cu caracter personal în țările „Parteneriatului pentru o bună guvernare" (PGG)

În aprilie 2014, Uniunea Europeană și Consiliul Europei au convenit printr-o declarație de intenție ca activitățile de cooperare vizate cu Armenia, Azerbaidjan, Georgia, Republica Moldova, Ucraina și Belarus - țările Parteneriatului estic al UE - să fie implementate în baza unui cadru specific de cooperare denumit în prezent PGG.

Unul dintre obiectivele generale ale acestui Program PGG este să „consolideze dreptul la protecția datelor".

1. Republica Armenia

Republica Armenia a semnat Convenția 108 la 8 aprilie 2011 și a ratificat instrumentul la 9 mai 2012.

La aceeași dată, aceasta a ratificat Protocolul adițional la Convenția 108 privind autoritățile de supraveghere și fluxul de date transfrontalier.

Constituția Armeniei conține o prevedere legată de protecția confidențialității (articolul 34).

Legea cu privire la protecția datelor cu caracter personal a fost adoptată de Parlamentul țării la 18 mai 2015 și a intrat în vigoare la 1 iulie 2015. Aceasta stabilește un cadru legal pentru prelucrarea datelor cu caracter personal de către sectorul public și cel privat.

Agenția pentru protecția datelor cu caracter personal din Armenia a fost înființată în anul 2015 pe baza Legii cu privire la protecția datelor cu caracter personal.

Aceasta este un organ administrativ care acționează în subordinea Ministerului Justiției din Republica Armenia și este responsabilă de supravegherea legalității modului de prelucrare a datelor cu caracter personal.

Agenția controlează și supraveghează implementarea legislației cu privire la protejarea datelor cu caracter personal și legitimitatea prelucrării datelor cu caracter personal[18].

Agenția este formată din 7 persoane (inclusiv Șeful Agenției) pentru o populație totală estimată de 3 milioane de persoane.

2. Republica Azerbaidjan

Republica Azerbaidjan a semnat și ratificat Convenția 108 la data de 3 mai 2010.

Articolul 32 din Constituție abordează subiectul protecției confidențialității.

În plus, a fost adoptată și o Lege privind „datele, prelucrarea datelor și protecția datelor"[19].

[18] http://www.moj.am/
[19] https://rm.coe.int/16806aef9d

Această lege definește politica statului privind sistemele informatice, tipurile, modurile și formele de colectare, precum și modul de folosire și protecția informațiilor.

Capitolul 5 din această lege reglementează aspecte legate de protecția datelor. Conform articolului 17, scopul protecției datelor constă din următoarele elemente:
• luarea unor măsuri preventive împotriva distrugerii, pierderii și falsificării datelor;
• siguranța statului, publicului și a cetățenilor;
• luarea unor măsuri preventive împotriva acțiunilor neautorizate legate de distrugerea, modificarea, copierea și izolarea datelor;
• protejarea confidențialității datelor care constituie secret de stat;
• asigurarea drepturilor persoanelor fizice și juridice în procesele informatice și la elaborarea, producerea și folosirea sistemelor informatice, tehnologiei și mijloacelor de susținere a acestora.

La data de 11 mai 2010, Republica Azerbaidjan a adoptat o lege „privind datele cu caracter personal" pentru reglementarea modului de colectare, prelucrare și protejare a datelor cu caracter personal, precum și a aspectelor legate de transferul transfrontalier de date cu caracter personal pentru definirea drepturilor și obligațiilor organelor publice și autorităților locale, persoanelor fizice și persoanelor juridice care activează în acest domeniu. Articolul 4 din această lege stabilește principiile de bază privind colectarea, prelucrarea și protecția datelor cu caracter personal.

Cabinetul Miniștrilor Republicii Azerbaidjan aprobă „Cerințele pentru protecția datelor cu caracter personal" pentru aplicarea „Legii privind datele cu caracter personal". Cerințele pentru protecția datelor cu caracter personal sunt implementate de următoarele autorități: Ministerul Comunicațiilor și Înaltelor Tehnologii; Serviciul Securității Statului; Ministerul Afacerilor Interne; Ministerul Justiției; Serviciul Special de Protecție al Statului.

Nu au fost stabilite autorități specifice independente de protecție a datelor.

3. Republica Belarus

Republica Belarus nu este membră a Consiliului Europei și nu este parte la Convenția 108.

Constituția Republicii Belarus este documentul fundamental pentru protecția datelor cu caracter personal. În concordanță cu articolul 28 din Constituție, orice persoană are dreptul la protecție împotriva ingerințelor nelegale în viața personală, inclusiv corespondența, comunicațiile telefonice și alte comunicații, onoare și demnitate.

Articolul 34 din Constituție prevede obligația autorităților centrale, asociațiilor publice și oficialităților de a acorda cetățenilor Republicii Belarus oportunitatea de a supune analizei materialele care le afectează drepturile și interesele legitime.

Acest articol mai stipulează și că folosirea informațiilor poate fi restricționată de cadrul legislativ pentru a proteja onoarea, demnitatea și viața familială a cetățenilor și pentru ca aceștia să-și poată exercita drepturile pe deplin.

Normele Constituției sunt dezvoltate în continuare în legea Republicii Belarus din 10 noiembrie 2008 „privind informațiile, informatizarea și protecția informațiilor”.

Articolul 1 din această lege definește conceptul de date cu caracter personal, care se referă la datele cu caracter personal ale unei persoane fizice, elementare și adiționale, care trebuie introduse în registrul de evidență a populației în concordanță cu legislația Republicii Belarus, precum și la alte date folosite pentru identificarea unei anumite persoane.

Articolul 18 mai stipulează și că colectarea, prelucrarea, stocarea și folosirea datelor cu caracter personal se poate face doar cu acordul scris al persoanei vizate, dacă nu este altfel prevăzut printr-un act normativ al Republicii Belarus.

Procedura folosită pentru a obține, colecta, prelucra, acumula, stoca, furniza și folosi informații despre viața privată și datele cu caracter personal ale unei persoane fizice este specificată prin actele normative ale Republicii Belarus.

Conform articolului 34 din textul legii, utilizatorii informațiilor au dreptul de a-și supune analizei datele cu caracter personal.

În plus, dată fiind absența unei legi cuprinzătoare pentru protecția datelor cu caracter personal, norma legală pentru protecția datelor cu caracter personal din Republica Belarus este administrată la nivelul legislației secundare, din care cea mai importantă este cea din 21 iulie 2008 „cu privire la registrul de evidență a populației”.

Această lege descrie conceptul de date cu caracter personal în scopul aplicării și definește lista datelor cu caracter personal incluse în registrul de evidență a populației, precum și procedura de lucru cu aceste informații.

În prezent, nu există o autoritate independentă pentru protecția datelor în Belarus.

Cu toate acestea, este posibilă elaborarea și adoptarea unei legi speciale privind datele cu caracter personal spre sfârșitul anului 2018 - începutul anului 2019.

4. Georgia

Georgia a semnat Convenția 108 la 21 noiembrie 2001 și a ratificat instrumentul la 14 decembrie 2005.

La data de 10 ianuarie 2014, a fost ratificat și Protocolul adițional la Convenția 108 privind Autoritățile de Supraveghere și Fluxurile Transfrontaliere de Date.

În **Georgia**, **Constituția din 1995** protejează dreptul persoanelor fizice la confidențialitate și secretul comunicațiilor, precum și a informațiilor conținute în evidențele oficiale legate de sănătatea, finanțele sau alte aspecte private ale unei persoane (conform articolelor 20 și 41).

Cadrul legislativ care face trimitere mai exact la protecția datelor este definit în principal de **Legea privind protecția datelor cu caracter personal** (Legea nr. 6325 din 25 mai 2012 din Georgia). Acest act normativ definește regulile și procedurile pentru prelucrarea datelor cu

caracter personal în Georgia și înființează Inspectoratul pentru Protecția Datelor cu Caracter Personal din Georgia.

Legea prevede principii de bază care vor fi urmate în prelucrarea datelor cu caracter personal și stabilește temeiurile specifice pentru legitimitatea prelucrării datelor. Există temeiuri separate pentru prelucrarea datelor generale cu caracter personal și pentru prelucrarea datelor sensibile. În plus, legea prevede reglementări specifice privind datele biometrice, supravegherea video și marketingul direct. Un capitol separat al legii privind protecția datelor cu caracter personal tratează obligațiile operatorilor de date, inclusiv, *inter alia,* obligația de a furniza informații persoanei vizate, de a asigura securitatea datelor și de a ține sistemul de evidență a datelor. Drepturile persoanei vizate sunt prevăzute și într-un capitol specific din lege. În baza reglementărilor curente, persoana vizată are dreptul de a cere informații sau de a cere completarea, corectarea, blocarea, distrugerea, ștergerea sau radierea datelor cu caracter personal, precum și dreptul de a face o contestație sau de a introduce o cale de atac.

Legea se aplică atât sectorului public, cât și celui privat. Obiectul său și mandatul inspectorului acoperă toate tipurile de prelucrare a datelor, cu următoarele excepții: (i) prelucrarea datelor în scopuri personale, (ii) prelucrarea datelor în scopul procedurilor judiciare, în măsura în care aceasta poate aduce atingere procedurii în sine; (iii) prelucrarea datelor în scopul securității de stat (inclusiv securității economice), apărării, în activități de informații și contrainformații, (iv) prelucrarea informațiilor cu caracter personal considerate ca secret de stat, cu excepția informațiilor prelucrate pentru prevenirea infracționalității, investigarea infracțiunilor, scopuri operativ-investigative și pentru protejarea ordinii publice[20].

Inspectoratul este format din 43 de persoane pentru o populație totală estimată de 3,7 milioane de persoane.

5. Republica Moldova

Republica Moldova a ratificat Convenția 108 la 28 februarie 2008 și Protocolul adițional la Convenție la 28 septembrie 2011.

Articolul 28 din Constituția de la 1994 protejează confidențialitatea și vizează protecția datelor cu caracter personal.

Prima lege privind protecția datelor cu caracter personal a fost Legea nr. 17-XVI din 15.2.2007, care a fost abrogată și înlocuită de Legea nr. 133 din 8.7.2011, care constituie actualmente documentul legal central privind protecția datelor cu caracter personal în Republica Moldova. Merită menționate alte două documente importante în acest sens: (1) Legea nr. 182-XVI din 10.7.2008 pentru aprobarea Regulamentului, structurii și finanțării Centrului Național pentru Protecția Datelor cu Caracter Personal, și (2) Legea nr. 229 din 10.10.2013 pentru aprobarea Strategiei naționale de dezvoltare în domeniul protecției datelor cu caracter personal pentru perioada 2013-2018 și a Planului de acțiune pentru implementarea acesteia.

[20] https://personaldata.ge/en/home

Centrul Național[21] pentru Protecția Datelor cu Caracter Personal din Republica Moldova (CNPDCP) a fost înființat în 2008, dobândind statutul de autoritate publică autonomă, independentă de alte autorități publice, persoane fizice și persoane juridice, conform prevederilor Convenției 108.

În prezent, CNPDCP este singura autoritate care poate veghea la respectarea drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, în mod notabil dreptul la intimitate, familie și viață privată, astfel cum este consacrat în articolul 28 din Constituția Republicii Moldova.

Un nou proiect de lege pentru consolidarea cadrului legal actual este în curs de elaborare.

Centrul este format din 16 persoane (inclusiv Directorul) pentru o populație estimată de 2,9 milioane de persoane.

Merită menționat faptul că organizarea internă curentă a Autorității de Protecție a Datelor va fi modificată semnificativ, o nouă lege fiind dezbătută actualmente în Parlament. Creșterea planificată a limitei de personal este de la 21 la 45 de membri ai personalului.

6. Ucraina

La data de 6 iulie 2010, **Ucraina** a ratificat Convenția 108 și Protocolul adițional la aceasta. La data de 1 ianuarie 2011 a intrat în vigoare Legea privind protecția datelor cu caracter personal în Ucraina.

Articolul 32 din Constituția de la 1996 protejează confidențialitatea și datele cu caracter personal.

Legea privind protecția datelor cu caracter personal din Ucraina a fost adoptată la 1 iunie 2010. De atunci, aceasta a fost modificată de nouă ori (23 februarie 2012, 20 noiembrie 2012, 16 mai 2013, 3 iulie 2013, 27 martie 2014, 13 mai 2014, 9 aprilie 2015, 3 septembrie 2015 și 6 decembrie 2016).

În conformitate cu amendamentele introduse de Legea Ucrainei „cu privire la modificarea anumitor acte legislative ale Ucrainei privind îmbunătățirea protecției datelor cu caracter personal", funcția de control asupra respectării legislației privind protecția datelor cu caracter personal este atribuită Comisarului pentru drepturile omului al Parlamentului ucrainean [22].

Secretariatul Comisarului pentru Drepturile Omului al Parlamentului ucrainean include o unitate structurală separată - un Departament pentru Protecția Datelor cu Caracter Personal.

Departamentul este format din 15 persoane pentru o populație estimată de 42,5 milioane de persoane.

[21] http://www.datepersonale.md/md/start/
[22] http://www1.ombudsman.gov.ua/en/

5. Obiectul acestui manual de formare

Scopul acestui Manual de Formare este să ofere o descriere generală a rolului și misiunii autorităților responsabile de protecția datelor.

Acesta este prevăzut a ajuta autoritățile de protecție a datelor nou înființate sau membrii noi ai acestor autorități să înțeleagă mai bine particularitățile și specificul autorităților de protecție a datelor.

Se pune un accent deosebit pe provocările care apar la instituirea autorității (motivele înființării unei autorități de protecție a datelor, cerințele privind independența, definirea unei strategii și a unui program de lucru, definirea unei structuri și a unei organigrame etc.).

Apoi, este descris cu atenție rolul consultativ al autorității de protecție a datelor. Acest rol devine din ce în ce mai diversificat, iar autoritatea de protecție a datelor ar putea fi implicată cu privire la mai multe aspecte: proceduri de notificare și de autorizare; opinii cu privire la proiecte de legi; definirea de modele și orientări la nivel sectorial; elaborarea de instrumente de responsabilizare (responsabili cu protecția datelor, registre, evaluarea impactului asupra confidențialității, certificare, coduri de conduită etc.); stabilirea de relații cu cercuri de cercetare și inovare etc.

Apoi, acest manual de formare abordează competențele de supraveghere ale unei autorități de protecție a datelor. Acesta va descrie competențele *ex post* ale autorității: soluționarea plângerilor persoanelor; verificările operatorilor; adoptarea sancțiunilor; capacitatea de a aduce un caz în atenția autorităților judiciare.

De asemenea, este abordată nevoia de a institui o strategie de comunicare și de a derula campanii de sensibilizare.

În final, sunt descrise activitățile de cooperare și cele internaționale ale autorităților.

Dacă este posibil și dacă sunt resurse disponibile în limba engleză, acest manual de formare încearcă să ofere exemple care derivă din experiențele țărilor vizate, respectiv Armenia, Azerbaidjan, Belarus, Georgia, Moldova și Ucraina. Întrucât Azerbaidjan și Belarus nu au înființat autorități de protecție a datelor la momentul elaborării acestui manual de formare, se vor face mai puține referiri la experiența acestor două țări.

Atunci când nu există resurse disponibile în limba engleză din experiențele țărilor vizate, acest manual de formare va oferi, de asemenea, exemple din alte țări.

Obiectivul general este și partajarea de **bune practici** care au fost dezvoltate de diferite autorități pentru protecția datelor. Acest manual poate constitui un set de unelte pentru autoritățile nou-înființate sau autoritățile cu experiență care caută informații pe un anumit subiect.

Trebuie reamintit, în același timp, că rolul și misiunile autorităților responsabile de protecția datelor depind în primul loc de legislația națională. Legislația națională este cea care definește domeniul de aplicare și întinderea competențelor unei autorități responsabile de protecția datelor.

Este posibil ca unele misiuni descrise în acest manual să nu fie încadrate în sfera de competență a unei anumite autorități de protecție a datelor.

Trebuie reținut că misiunile descrise în acest manual reflectă posibilele misiuni ale autorităților de protecție a datelor în general și nu reflectă misiunile și competențele reale ale fiecărei astfel de autorități în parte din țările vizate.

PARTEA 1: ÎNFIINȚAREA AUTORITĂȚII PENTRU PROTECȚIA DATELOR

Aproape toate statele membre ale Consiliului Europei au adoptat legislații naționale specifice privind protecția datelor, definind principiile de protecție a drepturilor omului în ceea ce privește prelucrarea datelor cu caracter personal.

Deoarece principiile prevăzute de lege sunt generale și ample în ceea ce privește natura lor (proporționalitate, limitarea scopului, calitatea datelor, securitatea etc.), în timp ce riscurile sunt diverse și depind de circumstanțele specifice fiecărui caz, există nevoia de **supraveghere externă din partea unei autorități imparțiale și calificate pentru a se ajunge la un echilibru corect între interesele conflictuale**, și anume necesitatea ca operatorii să prelucreze date personale și necesitatea de a proteja viața privată a persoanelor.

Este necesar să se stabilească o autoritate specifică care să dispună de misiuni și competențe pentru a pune în aplicare pe deplin principiile generale de protecție a datelor, să elaboreze recomandări privind categoriile de prelucrare a datelor cu caracter personal sau chiar să autorizeze o prelucrare a datelor cu risc deosebit pentru a elabora orientări, și să monitorizeze activitățile operatorilor de date și evoluția tehnologiilor informației și comunicațiilor.

În plus, având în vedere volumul de date prelucrate, numărul de posibile persoane afectate și peisajul tehnologic care se dezvoltă rapid, această necesitate poate fi satisfăcută într-un mod mai reactiv și detaliat de către o autoritate independentă și imparțială decât prin adoptarea unui cadru de reglementare sau printr-un răspuns judiciar.

O autoritate de protecție a datelor poate aduce flexibilitatea și reactivitatea necesară la provocările pe care le prezintă era digitală.

Deoarece autoritatea de supraveghere trebuie să monitorizeze și activitatea de prelucrare a organismelor publice, această autoritate va fi complet independentă și imparțială.

1. Obligația de a înființa o autoritate de protecție a datelor și modele existente

1. Protocolul adițional la Convenția 108

Protocolul adițional la Convenția 108 prevede că părțile vor înființa una sau mai multe autorități care să fie responsabile de asigurarea conformității cu măsurile prevăzute de dreptul intern, punând în aplicare principiile Convenției și ale acestui Protocol.

Protocolul adițional nu prescrie un model specific de autoritate pentru protecția datelor, dar prevede că:

- autoritățile de supraveghere au competențele de investigație și intervenție, precum și competența de a se angaja în proceduri judiciare sau de a aduce la cunoștința autorităților judiciare competente încălcări ale prevederilor dreptului intern;
- fiecare autoritate de supraveghere audiază cererile depuse de orice persoană cu privire la protecția drepturilor și a libertăților fundamentale ale acesteia în ceea ce privește prelucrarea datelor cu caracter personal care țin de competența sa;
- autoritățile de supraveghere își exercită funcțiile în deplină independență;
- deciziile autorităților de supraveghere, care dau naștere la plângeri, pot fi contestate în instanță.

2. La nivel național

La nivel național există mai multe modele pentru protecția datelor. În unele țări, mai multe modele sunt folosite simultan.

Modelul de reglementare adoptat de țările europene, Australia, Noua Zeelandă sau Canada constă în instituirea unui *organism de drept public* care să aplice o lege cuprinzătoare cu privire la protecția datelor.

Unele țări, cum ar fi Statele Unite, au evitat legislația generală privind protecția datelor în favoarea unor *legi sectoriale* specifice care reglementează, de exemplu, evidențele închirierii de materiale video, protecția vieții private a copiilor sau confidențialitatea financiară.

În alte țări, legile sectoriale sunt utilizate pentru a completa legislația exhaustivă, oferind protecții mai detaliate pentru anumite categorii de informații, cum ar fi dosarele de poliție sau evidența creditelor de consum.

Unele țări încurajează, de asemenea, diferite forme de auto-reglementare, în care societățile și organismele din industrie stabilesc coduri de bună practică.

Agenția UE pentru Drepturi Fundamentale a publicat un raport privind rolul autorităților de protecție a datelor. Raportul prevede că, în Europa, unele state au desemnat o autoritate de protecție a datelor cu competențe generale și alte câteva organisme de supraveghere specifice sectorului (de exemplu, în domeniul sănătății, poștei sau telecomunicațiilor). Unele dintre aceste state organizate de-a lungul liniilor federale sau cu puteri semnificative deținute la nivel regional sunt înzestrate, la rândul lor, cu un organism național de supraveghere și cu mai multe agenții sub-statale cărora li se încredințează aceeași funcție la nivel regional sau federal. În plus, în timp ce în multe țări, înainte de înființarea autorităților de protecție a datelor, datoria de a monitoriza respectarea drepturilor de confidențialitate a fost încredințată instituțiilor Ombudsmanului, în unele state membre, Ombudsmanul continuă să dețină o funcție relevantă în ceea ce privește protecția datelor cu caracter personal.[23]

[23] http://fra.europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities

3. Modele

În ceea ce privește alcătuirea autorităților de protecție a datelor, două modele principale pot fi observate în țările europene: un model colegial și modelul comisarului unic.

Modelul colegial

Modelul colegial este larg răspândit, dar nu cel mai frecvent utilizat model. De exemplu, în Austria, Belgia, Bulgaria, Franța, Italia, Grecia, Luxemburg, Olanda sau Portugalia există o autoritate colegială de protecție a datelor. Modelul colegial poate fi găsit și în Burkina Faso, Quebec, Mexic, Monaco, Maroc, Tunisia, Senegal sau Uruguay.
Pluralismul și calificarea membrilor unui organ colegial depind de numirea membrilor care reprezintă diverse medii și circumscripții și de capacitatea membrilor de a trata drepturile omului și problemele tehnologice.

În Uniunea Europeană, numărul membrilor variază de la trei în Luxemburg și Olanda, la patru în Italia, la mai mult de zece în Portugalia și Grecia, și până la 17 în Franța.

De exemplu, autoritatea franceză de protecție a datelor, CNIL, este compusă din patru parlamentari; doi membri ai Consiliului Economic, Social și de Mediu din Franța, șase reprezentanți ai unor jurisdicții înalte și cinci personalități calificate, numiți de Președintele Adunării Naționale, de Președintele Senatului și de Consiliul de Miniștri al Franței. Președintele CNIL este ales de către și din rândul membrilor.

În Belgia, Parlamentul alege membrii din rândul celor nominalizați de către Guvern. Guvernul este obligat să numească de două ori mai multe persoane decât numărul de membri care trebuie aleși.

Modelul comisarului unic

Modelul „comisarului unic" este aplicat în numeroase țări, uneori utilizând diferite proceduri care implică, de exemplu, un juriu independent *ad-hoc* înainte ca numirea să fie făcută de guvern sau de Parlament.
Desemnarea este făcută din ce în ce mai des de Parlament. În Germania, autoritatea federală de protecție a datelor a fost desemnată la început de către guvern, însă aceasta este aleasă acum de către Parlament. În landurile germane, comisarii sunt aleși și de parlamentele provinciilor.

Comisarul este deseori asistat de unul sau doi comisari adjuncți.
În ceea ce privește instituțiile Uniunii Europene, a fost instituită o procedură de selecție specifică pentru Autoritatea Europeană pentru Protecția Datelor și adjunctul Autorității Europene pentru Protecția Datelor:
- o invitație publică are ca rezultat intrarea pe lista scurtă a celor mai competenți candidați la decizia unei comisii de selecție interinstituționale;
- în urma interviurilor cu candidații selectați, comisia de selecție prezintă Comisiei Europene recomandările privind revizuirea și prezentarea lor Parlamentului European și Consiliului.
- în Parlamentul European sunt organizate audieri în vederea evaluării experienței, aptitudinilor și independenței candidaților;
- o decizie comună a Parlamentului și a Consiliului este adoptată în urma deliberărilor.

4. În țările PGG

În țările PGG, Armenia, Georgia, Moldova și Ucraina au optat pentru modelul de reglementare descris în continuare în acest manual.

În sfârșit, trebuie menționat faptul că unele autorități pentru protecția datelor au, de asemenea, competențe, conferite de legislația națională, în domeniul libertății de informare și al accesului la documentele publice.

În acest sens, nu există un model unic în Europa, deoarece unele țări au creat o autoritate specifică în domeniul libertății de informare, în timp ce alte țări au conferit unei autorități unice competența de a acționa atât în domeniul libertății de informare, cât și în cel al protecției datelor cu caracter personal.

2. Independența autorităților de protecție a datelor

Una din principalele cerințe pentru înființarea autorității este independența necesară pentru îndeplinirea misiunilor.

Independența va fi garantată, înainte de toate, în baza cadrului legal aplicabil.

De fapt, garanția independenței este asigurată, în primul rând, de procedura de numire și îndepărtare a membrilor de conducere ai autorităților de protecție a datelor. Bugetul devotat autorității de supraveghere și controlul asupra resurselor financiare reprezintă un al doilea element relevant în asigurarea autonomiei, independenței și eficienței autorităților de supraveghere.

1. Protocolul adițional la Convenția 108

Protocolul adițional la Convenția 108 statuează că autoritățile își vor exercita funcțiile în deplină independență.

În textul consolidat al propunerilor de modernizare a Convenției 108, finalizat de CAHDATA (ședința din 15-16 iunie 2016[24]), în articolul 12bis propus este indicat clar că:

„*4. Autoritățile de supraveghere acționează în deplină independență și imparțialitate în îndeplinirea sarcinilor și exercitarea competențelor lor și, în acest scop, nu solicită și nu acceptă instrucțiuni.*
5. Fiecare parte se asigură că autoritățile de supraveghere dispun de resursele necesare pentru îndeplinirea eficientă a funcțiilor lor și exercitarea competențelor lor”.

Modelul raportului explicativ[25] prevede că:

[24] Cf. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a616c
[25] https://rm.coe.int/16806b6ec2

„111. Prezentul articol vizează asigurarea unei protecții eficiente a persoanelor, solicitând părților să înființeze una sau mai multe autorități publice de supraveghere independente și imparțiale care contribuie la protecția drepturilor și libertăților persoanelor în ceea ce privește prelucrarea datelor lor cu caracter personal. Aceste autorități pot fi un comisar unic sau un organism colegial. Pentru ca autoritățile de supraveghere a protecției datelor să poată oferi o cale de atac adecvată, acestea trebuie să aibă competențe și funcții eficiente și să se bucure de o independență reală în îndeplinirea sarcinilor lor. Acestea reprezintă o componentă esențială a sistemului de supraveghere a protecției datelor într-o societate democratică. Se pot prevedea alte mecanisme adecvate pentru revizuirea și supravegherea independentă și eficientă a activităților de prelucrare, în măsura în care se aplică articolul 9 alineatul (3).

123. Alineatul (4) clarifică faptul că autoritățile de supraveghere nu pot proteja efectiv drepturile și libertățile individuale decât dacă își exercită funcțiile în deplină independență. O serie de elemente contribuie la protejarea independenței autorității de supraveghere în exercitarea funcțiilor sale, inclusiv a componenței autorității; metoda de numire a membrilor săi; posibilitatea acestora de a participa la reuniunile relevante fără restricții nejustificate; opțiunea de a consulta experți tehnici sau alți experți sau de a organiza consultări externe; durata exercitării și condițiile de încetare a funcțiilor; disponibilitatea unor resurse suficiente pentru autoritate; posibilitatea de a-și angaja propriul personal; sau adoptarea deciziilor fără a fi supuse unor interferențe externe, directe sau indirecte.

124. Interzicerea solicitării sau acceptării instrucțiunilor acoperă îndeplinirea sarcinilor ca autoritate de supraveghere. Acest lucru nu împiedică autoritățile de supraveghere să solicite consultanță specializată atunci când este considerată necesară, atâta timp cât autoritățile de supraveghere își exercită propria judecată independentă."

2. Uniunea Europeană

În **Uniunea Europeană**, cerința ca autoritățile de protecție a datelor să fie independente este prevăzută în special prin articolul 16 alineatul (2) din Tratatul privind Funcționarea Uniunii Europene (TFUE) și prin articolul 8 alineatul (3) din Carta Drepturilor Fundamentale.

Curtea de Justiție a Uniunii Europene a subliniat în mod constant că controlul exercitat de o autoritate independentă este o componentă esențială a dreptului la protecție a datelor și a stabilit criteriile pentru o astfel de independență.

În special, în hotărârea Marii Camere (*Comisia Europeană c. Republicii Federale Germania*, 9 martie 2010, cauza C518 /07[26]), Curtea Europeană de Justiție a constatat în particular că:

- În ceea ce privește un organism public, termenul „independență" înseamnă, în mod normal, un statut care asigură faptul că organismul în cauză poate acționa complet liber, fără să primească instrucțiuni sau să fie pus sub presiune;

26 http://curia.europa.eu/juris/document/document.jsf?text=&docid=79752&pageIndex=0&doclang=RO&mode=lst&dir=&occ=first&part=1&cid=1137278

- nu există niciun element care să indice că cerința de independență se referă exclusiv la relația dintre autoritățile de supraveghere și organismele care fac obiectul supravegherii. Dimpotrivă, conceptul de „independență” este completat de adjectivul „complet”, care implică o putere de decizie independentă **de orice influență externă directă sau indirectă asupra autorității de supraveghere;**

- Garantarea independenței autorităților naționale de supraveghere este menită să asigure eficacitatea și fiabilitatea supravegherii conformității cu dispozițiile privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și trebuie interpretată în lumina acestui obiectiv. S-a stabilit să nu se acorde un statut special acestor autorități și reprezentanților acestora, decât pentru a consolida protecția persoanelor și a organismelor afectate de deciziile lor. Rezultă că, în exercitarea atribuțiilor lor, autoritățile de supraveghere trebuie să acționeze în mod obiectiv și imparțial. În acest scop, acestea trebuie să rămână libere de orice influență externă, inclusiv influența directă sau indirectă a statului [sau landurilor], și nu doar de influența organismelor supravegheate;

- simplul risc ca autoritățile care examinează statul să poată exercita o influență politică asupra deciziilor autorităților de supraveghere este suficient pentru a împiedica îndeplinirea independentă a sarcinilor acestora din urmă.

Curtea a subliniat, de asemenea, rolul esențial al autorităților independente de supraveghere în ceea ce privește controlul transferurilor internaționale către țări din afara UE.

Într-un alt caz privind Austria [a se vedea Hotărârea Curții (Marea Cameră)), 16 octombrie 2012, *Comisia Europeană c.Republicii Austria*, C614/10[27]), Curtea Europeană de Justiție a considerat că cerința de independență nu a fost întrunită cu privire la autoritatea austriacă de protecție a datelor în lumina următoarelor elemente:

- membrul de conducere al autorității de protecție a datelor este un funcționar federal supus supravegherii;

- biroul autorității de protecție a datelor este integrat în departamentele Cancelariei Federale; și

- Cancelarul federal are dreptul necondiționat la informații care acoperă toate aspectele activității autorității de protecție a datelor.

27 http://curia.europa.eu/juris/document/document.jsf?text=&docid=128563&pageIndex=0&doclang=RO&mode=lst&dir=&occ=first&part=1&cid=303091

3. Regulamentul general privind protecția datelor (RGPD)

Regulamentul general privind protecția datelor (RGPD) pune, de asemenea, accent pe importanța independenței.

Articolul 52 din RGPD prevede că:

„1. Fiecare autoritate de supraveghere beneficiază de independență deplină în îndeplinirea sarcinilor sale și exercitarea competențelor sale în conformitate cu prezentul regulament.

2. Membrul sau membrii fiecărei autorități de supraveghere, în cadrul îndeplinirii sarcinilor și al exercitării competențelor sale (lor) în conformitate cu prezentul regulament, rămâne (rămân) independent (independenți) de orice influență externă directă sau indirectă și nici nu solicită, nici nu acceptă instrucțiuni de la o parte externă.

3. Membrul sau membrii fiecărei autorități de supraveghere se abțin de la a întreprinde acțiuni incompatibile cu atribuțiile lor, iar pe durata mandatului, nu desfășoară activități incompatibile, remunerate sau nu.

4. Fiecare stat membru se asigură că fiecare autoritate de supraveghere beneficiază de resurse umane, tehnice și financiare, de un sediu și de infrastructura necesară pentru îndeplinirea sarcinilor și exercitarea efectivă a competențelor sale, inclusiv a celor care urmează să fie aplicate în contextul asistenței reciproce, al cooperării și al participării în cadrul comitetului.

5. Fiecare stat membru se asigură că fiecare autoritate de supraveghere își selectează personalul propriu și deține personal propriu aflat sub conducerea exclusivă a membrului sau membrilor autorității de supraveghere respective.

6. Fiecare stat membru se asigură că fiecare autoritate de supraveghere face obiectul unui control financiar care nu aduce atingere independenței sale și că dispune de bugete anuale distincte, publice, care pot face parte din bugetul general de stat sau național; Capitolul VI din RGPD prevede norme detaliate pentru constituirea și funcționarea autorităților independente de supraveghere, inclusiv prevederi privind resursele necesare pentru îndeplinirea eficientă a sarcinilor și autorităților acestora.”

4. Armenia

În **Armenia**, agenția de protecție a datelor cu caracter personal constituie un organ administrativ care acționează în subordinea Ministerului Justiției din Republica Armenia și este responsabilă de supravegherea legalității modului de prelucrare a datelor cu caracter personal.

5. Georgia

În **Georgia**, Inspectorul de Protecție a Datelor cu Caracter Personal este ales de Parlamentul Georgiei. Inspectorul nu este subordonat altei oficialități sau altui organism public. Orice influență exercitată asupra inspectorului sau orice ingerință în activitățile sale este interzisă și pedepsită prin lege. Inspectorul se bucură de garanții și imunități.

În ceea ce privește procesul electoral, candidații la postul de inspector sunt aleși de o comisie specială care include reprezentanți ai guvernului și ai organizațiilor societății civile.

Candidații sunt apoi prezentați primului-ministru care selectează cel puțin două persoane în Parlament în vederea alegerilor. În consecință, societatea civilă și puterea executivă sunt implicate, împreună cu Parlamentul, în procesul electoral.

6. Republica Moldova

În **Republica Moldova**, conform articolului 22 alineatul (1) din Legea nr. 133 din 8.7.2011 privind protecția datelor cu caracter personal, Centrul Național pentru Protecția Datelor cu Caracter Personal este condus de un Director, numit de Parlament, cu majoritatea voturilor parlamentarilor aleși, la propunerea Președintelui Parlamentului, o fracțiune parlamentară sau cel puțin 15 parlamentari, pentru un mandat de 5 ani, care poate fi reînnoit o singură dată.

7. Ucraina

În **Ucraina**, autoritatea pentru protecția datelor a fost mai întâi sub autoritatea guvernului și această competență a fost ulterior conferită Comisarului pentru drepturile omului, ales de Parlament. Statutul său este definit de articolul 101 din Constituția Ucrainei, Legea Ucrainei „privind Comisarul Parlamentului ucrainean pentru drepturile omului” și privind protecția datelor prin Legea Ucrainei „cu privire la protecția datelor cu caracter personal”.

În conformitate cu articolul 4 din Legea Ucrainei „privind Comisarul Parlamentului ucrainean pentru drepturile omului”, comisarul își îndeplinește îndatoririle în mod independent de alte organe de stat și funcționari. Pentru realizarea efectivă a competențelor în domeniul protecției datelor, în cadrul Secretariatului Comisarului a fost creat Departamentul pentru Protecția Datelor cu Caracter Personal.

8. Resursele și mijloacele autorității

În ceea ce privește **resursele și mijloacele autorității**, care reprezintă o condiție pentru o independență și eficiență deplină, autoritățile de protecție a datelor trebuie să primească resursele necesare pentru funcționarea acestora. În majoritatea statelor, resursele financiare sunt alocate din bugetul statului pe o linie specifică și adesea din bugetul alocat Ministerului Justiției.

Cu toate acestea, în câteva state, autoritățile de supraveghere pot să-și mărească în mod semnificativ resursele financiare prin veniturile obținute din notificările făcute de către operatori cu privire la operațiunile lor de prelucrare a datelor și/ sau sancțiunile monetare impuse pentru încălcarea legislației privind protecția datelor (de exemplu, Luxemburg, Malta).

În Regatul Unit, taxele de notificare reprezintă singura sursă de venit pentru activitatea de protecție a datelor cu caracter personal a autorității de supraveghere.

În multe țări, lipsa unui nivel adecvat de finanțare a autorităților de supraveghere este subliniată ca o problemă[28].

Alocarea bugetului necesar instituției este necesară pentru a asigura independența materială a autorității și eficiența acesteia.

Autoritatea ar trebui, în special, să poată recruta angajați cu o înaltă specializare.

Destul de des, resursele umane necesare nu sunt disponibile și autoritățile ar trebui să fie în măsură să pregătească noi membri ai personalului pentru noi competențe care implică cunoștințe tehnice, manageriale și juridice.

De asemenea, autoritatea ar trebui să beneficieze de facilități suficiente și să obțină echipamente IT moderne, echipamente software și hardware de bună calitate necesare pentru îndeplinirea funcțiilor de bază: găzduirea unui site web pentru furnizarea de informații la nivel național și internațional, păstrarea unui registru al colecțiilor de date cu caracter personal și operațiuni de prelucrare, calculatoare pentru angajați, mijloace tehnice de primire și direcționare a plângerilor și pentru inspecții, de testare a noilor tehnologii, de cooperare cu alte autorități de protecție a datelor, de deplasare în străinătate la întâlniri etc.

[28] http://fra.europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities

3. Structura autorității de protecție a datelor

Alegerea unei structuri este o decizie-cheie pentru înființarea unei autorități de protecție a datelor.

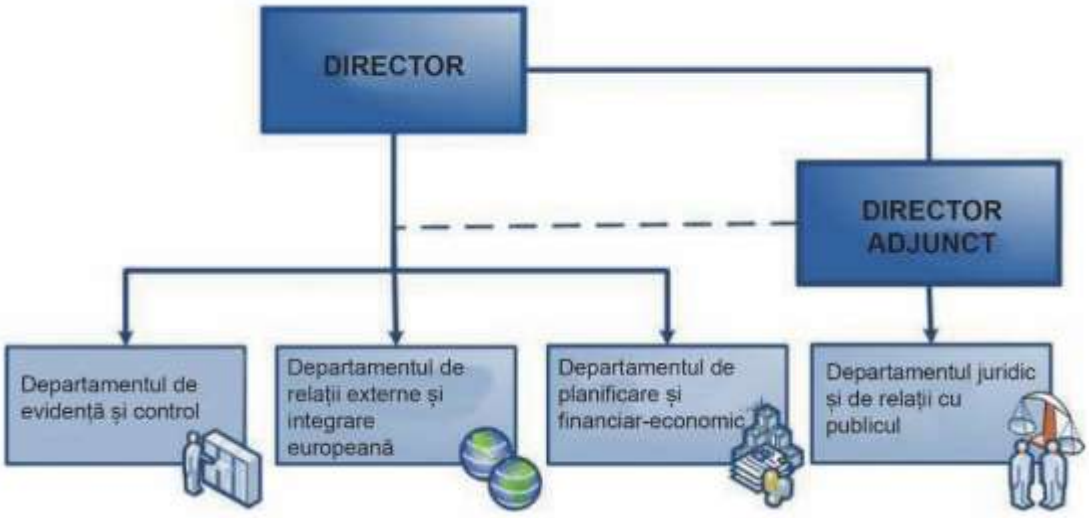
Alegerea structurii depinde în mare măsură de contextul local, de mijloacele și de experiența organizației sau de provocările specifice de la nivel național.

Mai jos sunt date câteva exemple de structuri existente ale autorităților de protecție a datelor.

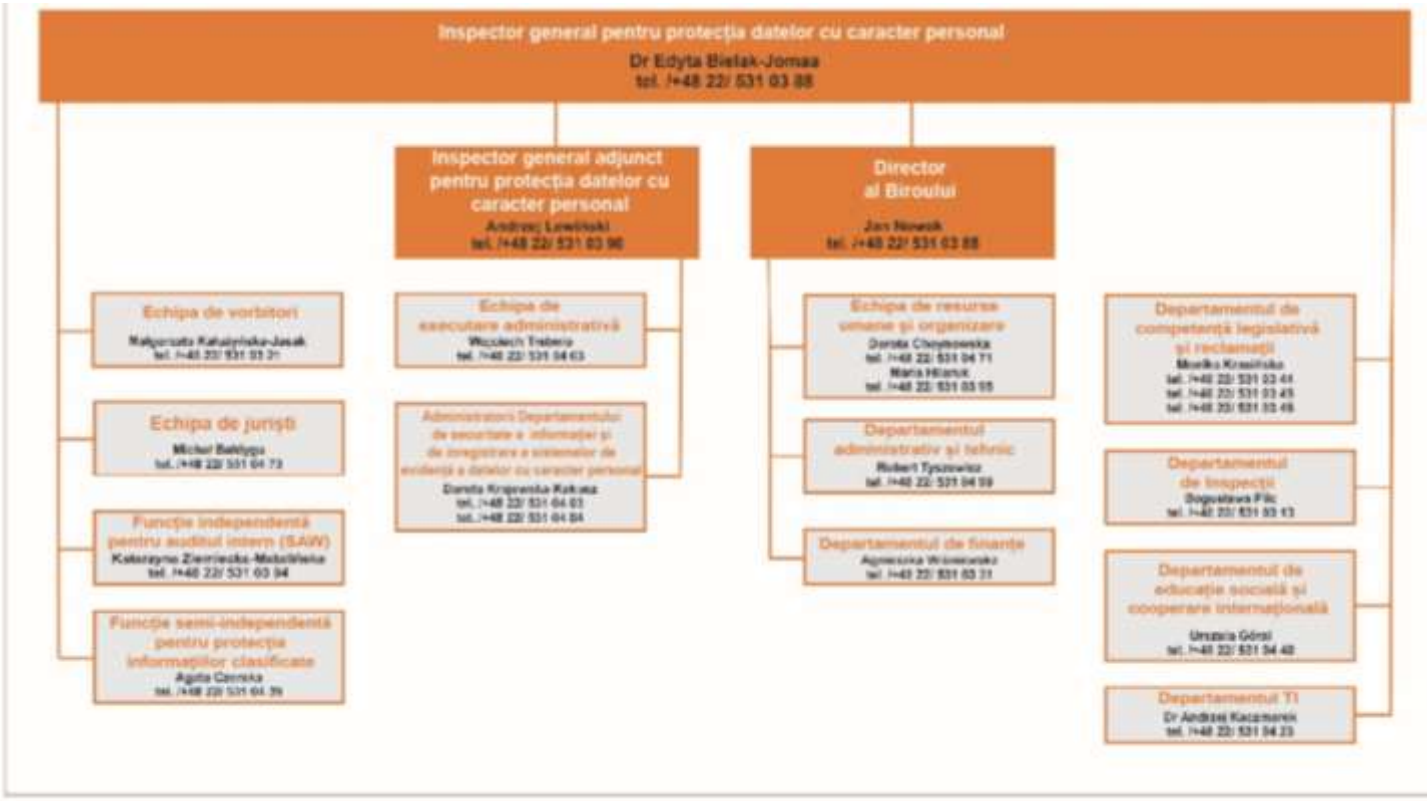
Exemplul 1: **Autoritatea de protecție a datelor din Georgia, iunie 2017**

Departamentul de inspecție este responsabil pentru investigațiile privind legitimitatea prelucrării datelor. Dacă se constată o încălcare a legii, decizia privind sancțiunile se face de către inspector pentru a separa competența de investigare de competența de sancționare. Departamentul juridic este responsabil pentru gestionarea reclamațiilor persoanelor.

Exemplul 2: **Autoritatea de protecție a datelor din Republica Moldova, iunie 2017**

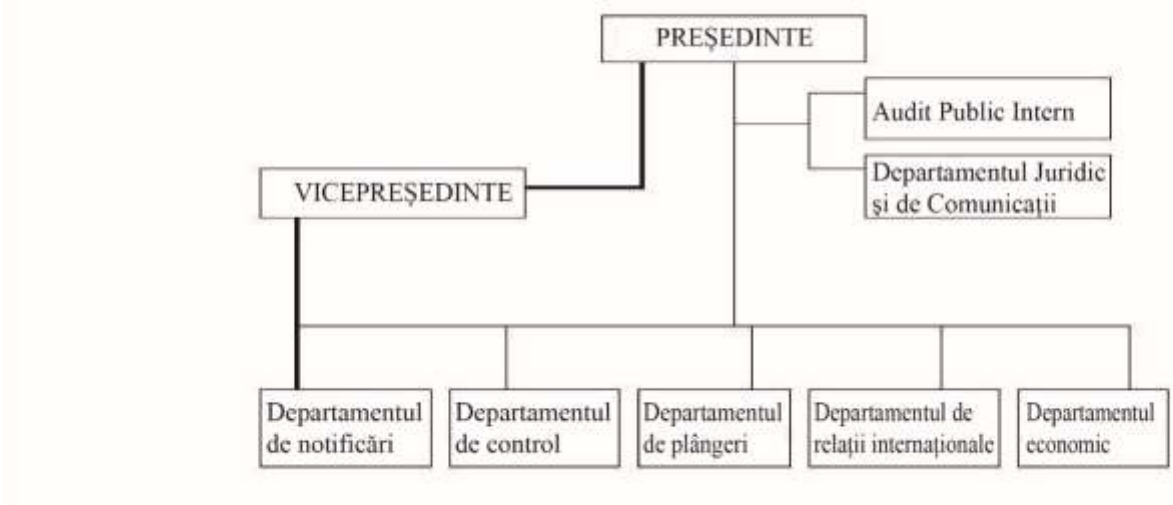


Exemplul 3: Autoritatea de protecție a datelor din Polonia, iunie 2017

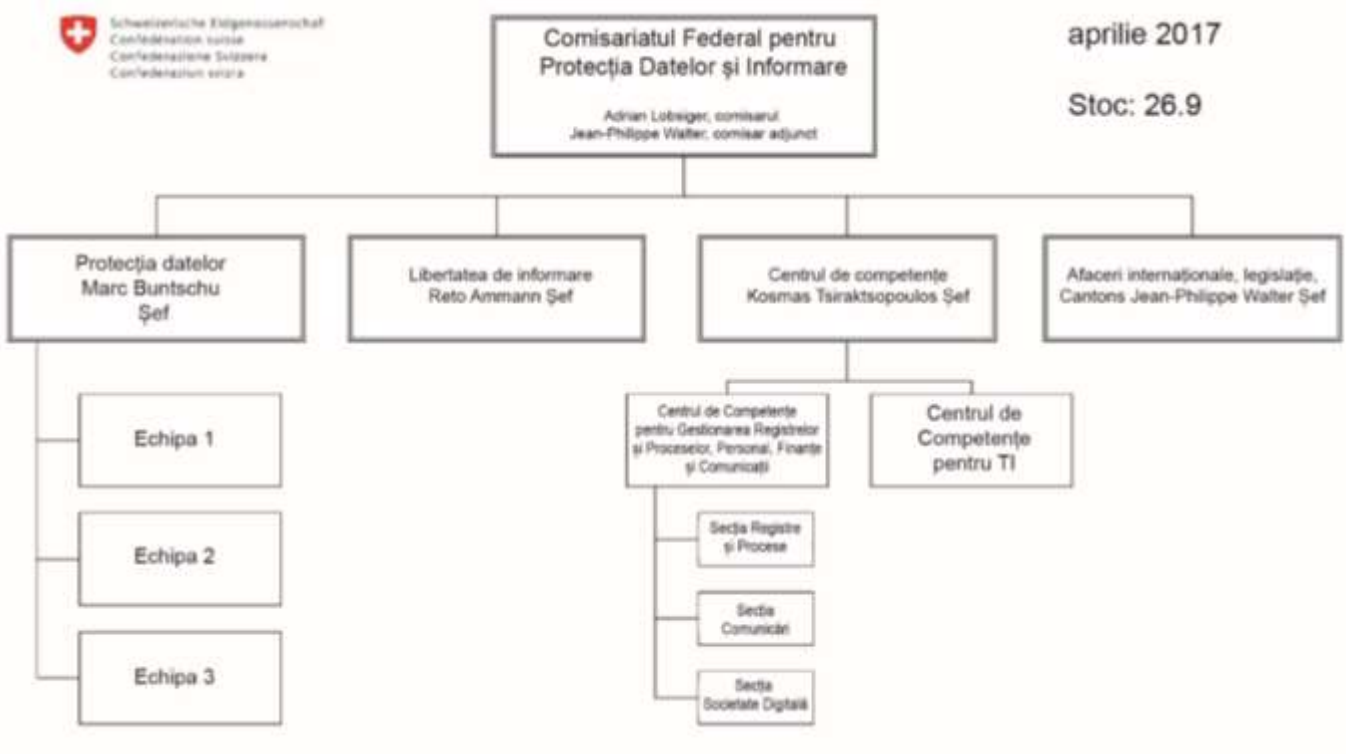


Exemplul 4: Departamentul de Protecție a Datelor cu Caracter Personal din cadrul Comisiei pentru drepturile omului, Ucraina

Exemplul 5: Autoritatea de protecție a datelor din România, iunie 2017



Exemplul 6: Autoritatea de protecție a datelor din Elveția, aprilie 2017



4. Definirea strategiei și a priorităților instituției

1. Priorități

Misiunea generală a unei autorități pentru protecția datelor este să pună în aplicare principiile generale de protecție a datelor și să asigure o protecție eficientă a persoanelor cu privire la prelucrarea datelor cu caracter personal, permițând totodată libera circulație a informațiilor.

Având în vedere mijloacele umane și financiare limitate și evoluția rapidă a contextului tehnologic, autoritățile de protecție a datelor trebuie **să definească anumite priorități și să identifice provocările cheie pe care le vor aborda.**

Obiectivul general este crearea unui cerc virtuos pentru un cadru durabil de protecție a datelor.

În faza de înființare a unei autorități, prima prioritate este în general instalarea noii unități și a sediului instituției.

Autoritatea va trebui, de asemenea, să se implice în activități privind resursele umane. Trebuie definite profilurile membrilor conducerii. Alți membri ai personalului ar trebui să fie recrutați într-o a doua fază, cu axare-pe diferite competențe și profiluri (conducere, consilieri juridici și IT, personal administrativ și de suport, etc.).

Membrii personalului trebuie să fie instruiți și trebuie să li se ofere oportunități de evoluție în carieră.

2. Strategie

În ceea ce privește strategia, în funcție de competențele lor și de dezbaterile naționale care au avut loc în timpul adoptării legislației privind protecția datelor, unele autorități pentru protecția datelor au optat pentru un rol preventiv și proactiv, subliniind rolul lor *ex-ante* în asigurarea protecției datelor cu caracter personal. Alte autorități au acordat prioritate aplicării legislației și controlului *ex-post* .

Natura competențelor atribuite organismelor de supraveghere poate, prin urmare, să varieze în mod corespunzător, existând preferința pentru instrumentele de prevenire neobligatorii în primele cazuri și pentru măsurile mai „dure” în celelalte cazuri[29].

3. Punerea în aplicare a legislației privind protecția datelor

În ceea ce privește punerea în aplicare a legislației privind protecția datelor, autoritățile de protecție a datelor nu dispun, de obicei, de mijloace pentru a viza în același timp toate sectoarele de activitate.

Multe autorități de protecție a datelor aleg să se axeze pe anumite domenii și sectoare specifice.

Ar trebui analizate punctele forte, punctele slabe și amenințările specifice ale unei țări.

Atenția și eforturile unei autorități de protecție a datelor se pot concentra asupra domeniilor care prezintă cel mai mare risc de neconformitate sau în care impactul asupra vieții private și protecției datelor este cel mai mare.

Pe baza constatărilor autorităților, ar trebui identificate priorități.

În primii ani, multe autorități acordă prioritate activităților de sensibilizare a persoanelor, operatorilor (pe sectoare de activitate) și persoanelor împuternicite de operatori. Una dintre primele provocări ale unei autorități este să fie identificată și recunoscută în țara sa.

De asemenea, strategia trebuie actualizată revizuită și complementată în mod constant.

4. Sensibilizare

După sensibilizarea persoanelor cu privire la prelucrarea datelor cu caracter personal și la protecția datelor, pot fi folosite sondaje pentru a identifica problemele cele mai stringente dintr-o țară:

Această metodă a fost folosită, de exemplu, în Armenia.

Exemplu: Sondaj desfășurat în Armenia

Care este cea mai stringentă problemă în domeniul protecției datelor cu caracter personal în Armenia?

Camerele video din spații publice și private	34 %
- Publicitatea prin mesaje text în rețeaua de telefonie mobilă	16 %
- Protecția datelor personale în relațiile de muncă	17 %
- Protecția datelor privind starea de sănătate a persoanelor	16 %
- Protecția datelor cu caracter personal ale minorilor	17 %

Tot în Armenia, Agenția și-a concentrat activitățile, în primul an de activitate, asupra a trei domenii prioritare, și anume: utilizarea datelor de supraveghere video, diseminarea mesajelor electronice nesolicitate și protecția copiilor. Agenția a elaborat și a adoptat Ghidul de supraveghere video care nu este obligatoriu, dar este recomandat pentru a fi utilizat de către toate entitățile care efectuează prelucrarea prin supraveghere video.

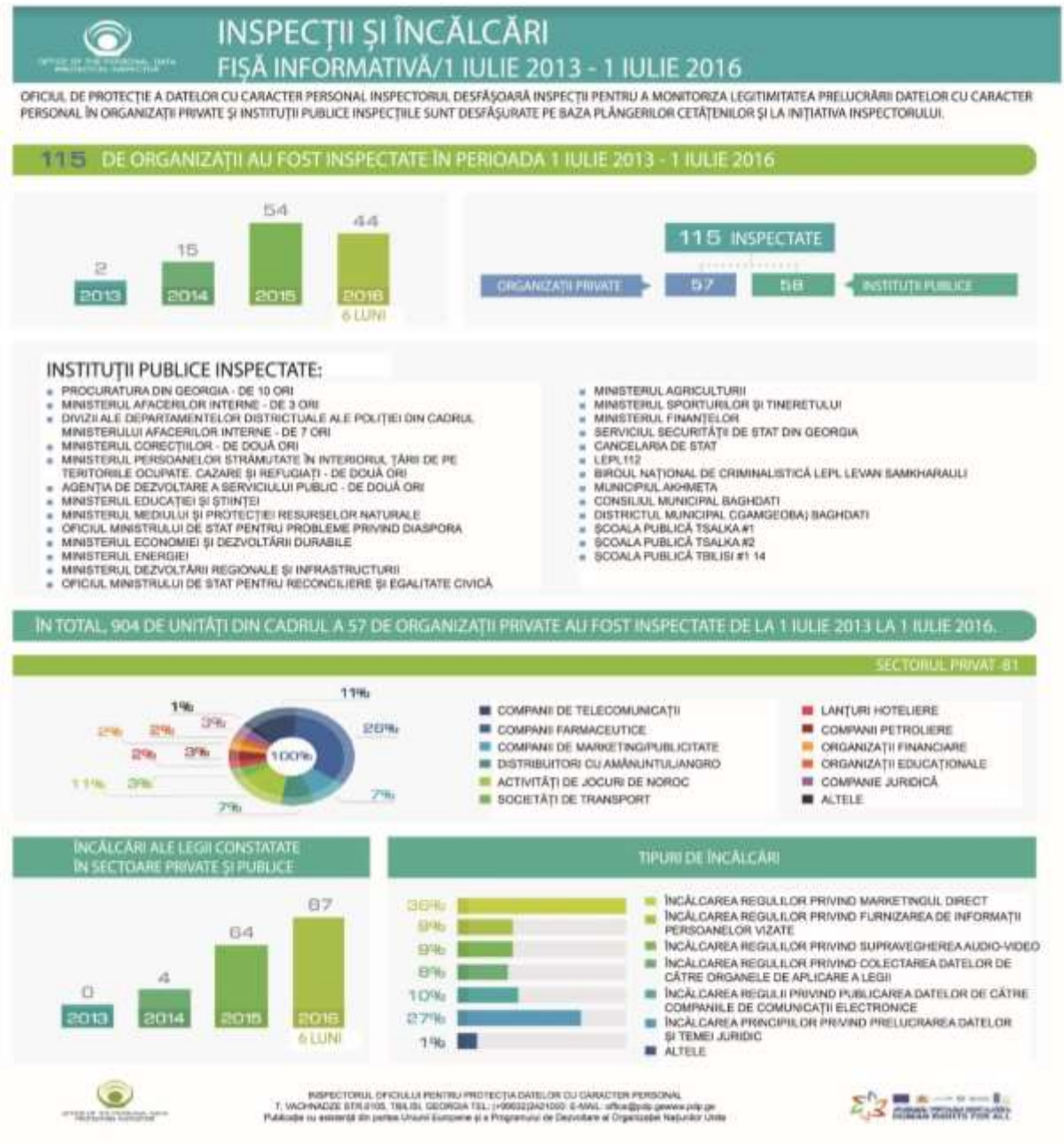
Și natura plângerilor primite de autoritățile de protecție a datelor poate contribui la identificarea problemelor-cheie.

5. Georgia

În **Georgia**, au fost elaborate o strategie de dezvoltare instituțională 2017-2021 și un plan de acțiune pentru 2017-2018 pentru Oficiul pentru protecția datelor cu caracter personal. În acest proces au fost definite misiunea, viziunea, valorile, obiectivele strategice și obiectivele asociate.

Analiza inspecțiilor întreprinse de autoritatea georgiană de protecție a datelor în primii trei ani de activitate indică faptul că principalele domenii de neconformitate în sectorul privat se referă la societăți de marketing direct, servicii de comunicații electronice, supraveghere audio sau video etc.

Conform strategiei, în 2017-2020, obiectivele principale ale Oficiului sunt de a iniția activitatea în domenii majore și de a spori eficacitatea Agenției prin dezvoltare organizațională, dar și promovarea sensibilizării publice și dezvoltarea în continuare a parteneriatelor strategice[30].



[30] https://personaldata.ge/en/personalur-monatsemta-datsvis-inspeqtoris-aparatma-2017-2021-tslis-strategia-partniorebsa-da-samoqalaqo-sazogadoebas-tsarudgina/667

6. Republica Moldova

Autoritatea de protecție a datelor din **Moldova** și-a publicat, de asemenea, lista de priorități și strategii[31]. Nevoia de a consolida capacitățile instituției și de a promova conceptul de protecție a datelor este identificată drept prioritate.

La data de 10 octombrie 2013, Parlamentul a adoptat Strategia națională de dezvoltare în domeniul protecției datelor cu caracter personal pentru perioada 2013-2018 și Planul de acțiune pentru implementarea acesteia.

Situația actuală privind punerea în aplicare a acestei strategii și a Planului de acțiune este, de exemplu, prezentată în raportul anual al instituției pe anul 2016.

Acesta descrie în special obiectivele instituției. Obiectivul general este asigurarea unui nivel adecvat de protecție a datelor cu caracter personal în Republica Moldova.

Acest Obiectiv general este împărțit în obiective specifice, după cum urmează:

- **Obiectivul specific 1.** Informarea tuturor operatorilor de date cu caracter personal cu privire la responsabilitățile lor, precum și la necesitatea de a proteja datele cu caracter personal prelucrate, ținând seama de cele mai recente tehnici în legătură cu riscurile care decurg din prelucrarea datelor cu caracter personal și natura datelor protejate:
  - Implicarea organizațiilor profesionale ale judecătorilor, executorilor judecătorești, avocaților, notarilor, băncilor, presei, sindicatelor, IT etc. pentru promovarea înregistrării în Registrul operatorilor de date cu caracter personal, precum și elaborarea codurilor de conduită profesională care să includă dispoziții referitoare la protecția datelor cu caracter personal sau să completeze codurile cu astfel de reguli;
  - acoperirea în mass-media a cazurilor cu rezonanță deosebită și a încălcărilor admise de entitățile de drept public și privat în prelucrarea datelor cu caracter personal;
  - acordarea de asistență instituțiilor publice și private, care sunt înființate ca operatori de date cu caracter personal, pentru a asigura respectarea procedurilor organizatorice și tehnice pentru protecția datelor cu caracter personal;
  - asigurarea de măsuri pentru acordarea de asistență controlorilor de date cu caracter personal la dezvoltarea declarațiilor de confidențialitate ca o clauză contractuală sau pentru a fi introduse în fișa postului, cu menționarea răspunderii civile, contravenționale sau penale în cazul încălcării unor astfel de declarații pentru persoanele care participă la procesul de prelucrare a datelor cu caracter personal;
  - revizuirea categoriilor și a cantității de date cu caracter personal prelucrate de operatori;
  - acordarea de asistență metodologică subdiviziunilor/ persoanelor responsabile de protecția datelor cu caracter personal stabilite în cadrul operatorilor de date cu caracter personal;
  - abordarea principiilor protecției datelor cu caracter personal, începând cu dezvoltarea sistemelor informatice și a sistemelor de evidență a datelor, destinate

[31] http://www.datepersonale.md/md/pdp/

prelucrării automate a datelor cu caracter personal (protejarea vieții private din faza de proiectare);

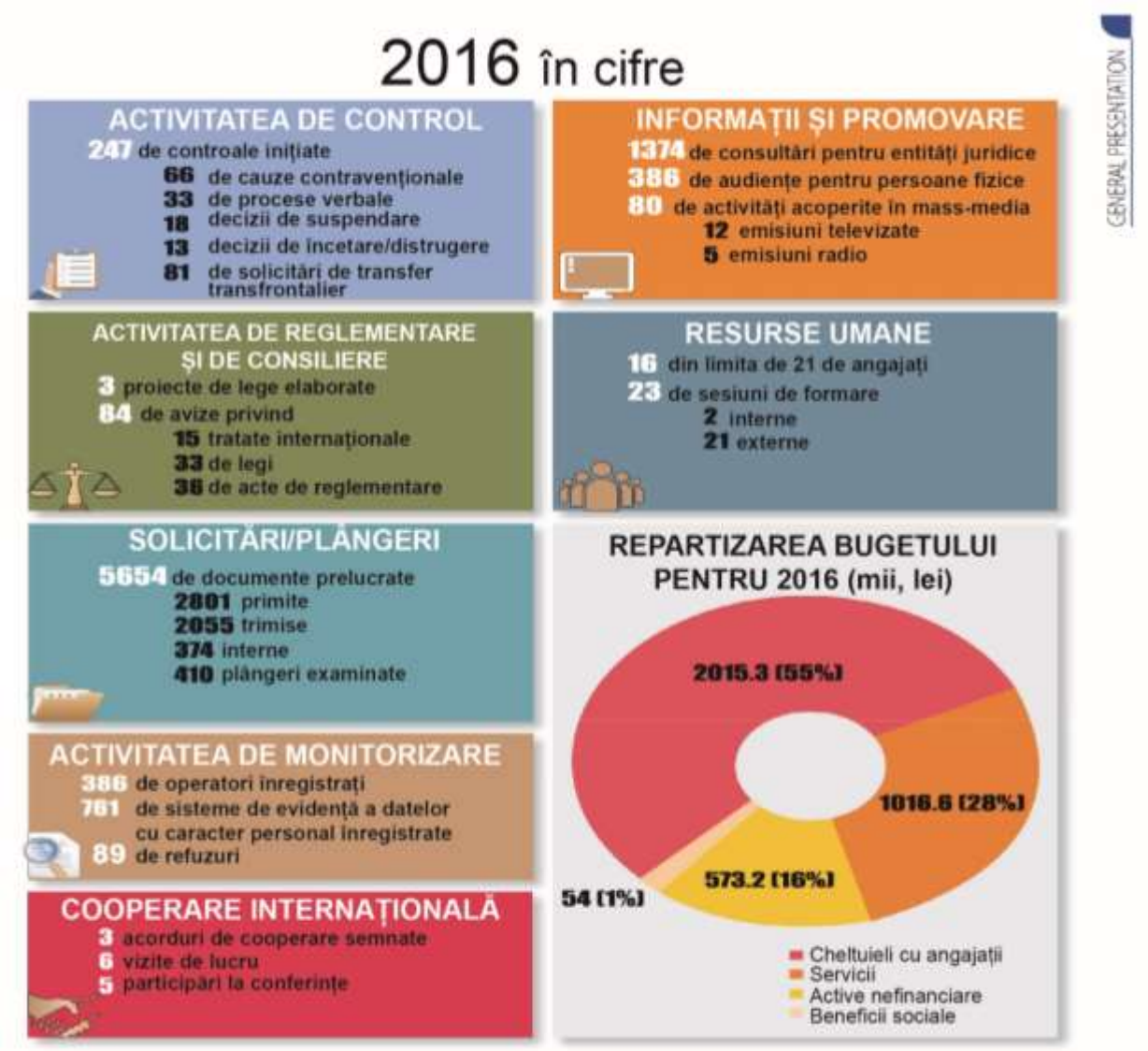
- acoperirea în mass-media, promovarea și monitorizarea respectării obligației de a notifica și înregistra operatorii de date cu caracter personal, bazele de date, sisteme informatice și sisteme IT care stochează și prelucrează date cu caracter personal, în mod automat sau manual, precum și respectarea principiului transparenței în activitatea de prelucrare a datelor.

- **Obiectivul specific 2.** Sensibilizarea publicului larg cu privire la drepturile pe care le are în legătură cu prelucrarea datelor cu caracter personal:
  - Implicarea activă a reprezentanților societății civile, a autorităților din învățământ și mass-media în sensibilizarea persoanelor cu privire la conceptele de „viață privată", „date cu caracter personal", beneficiile rezultate din protecția datelor cu caracter personal, consecințele negative care pot apărea atunci când regimul de prelucrare a datelor cu caracter personal, confidențialitatea și securitatea nu este respectată, precum și rolul protecției datelor cu caracter personal în dezvoltarea economică, socială și culturală a țării;
  - Organizarea de cursuri de formare pentru jurnaliști în legătură cu necesitatea de a asigura un echilibru între dreptul la libertatea de exprimare și dreptul la viață privată;
  - Organizarea de conferințe axate pe necesitatea respectării principiilor protecției datelor cu caracter personal;
  - Organizarea și implementarea evenimentelor naționale dedicate Zilei pentru protecția datelor cu caracter personal.

- **Obiectivul specific 3.** Crearea capacităților administrative și instituționale ale Centrului Național pentru Protecția Datelor cu Caracter Personal din Republica Moldova:
  - analiza modului în care sunt puse în aplicare deciziile emise de Centru în timpul controalelor întreprinse pentru a identifica problemele și deficiențele apărute;
  - analiza revendicărilor și plângerilor prezentate Centrului pentru a identifica problema și acțiunile necesare care trebuie întreprinse pentru a îmbunătăți situația în ceea ce privește protecția persoanelor relativ la prelucrarea datelor cu caracter personal, precum și protecția dreptului la intimitate, familie și viața privată;
  - revizuirea și avizarea cadrului normativ sectorial în concordanță cu principiile protecției datelor cu caracter personal;
  - formare continuă, schimb de experiență cu alte instituții europene similare, participarea la seminarii, cursuri, vizite de studiu, ateliere și conferințe internaționale;
  - asigurarea participării la forurile internaționale ale autorităților naționale care supraveghează protecția datelor cu caracter personal, promovarea imaginii Centrului și a celei a țării, precum și participarea activă în dezvoltarea cadrului normativ care reglementează domeniul protejării datelor cu caracter personal;
  - asigurarea informării publicului cu privire la problemele identificate în timpul controlului asupra modului în care legislația este respectată în ceea ce privește protecția datelor cu caracter personal.

În Moldova, descrierea activității Centrului Național pentru Protecția Datelor cu Caracter Personal reflectă, de asemenea, strategia și organizarea instituției.

Următoarele elemente reprezintă un extras al raportului anual al instituției pe anul 2016[32]:



7. Uniunea Europeană

Luând exemplul Uniunii Europene, Autoritatea Europeană pentru Protecția Datelor (AEDP), care a fost înființată în 2001, și-a adoptat Strategia pentru perioada 2015-2019[33].

Aceasta a identificat trei obiective strategice și numeroase acțiuni pentru a le duce la îndeplinire:

- „Protecția datelor devine digitală": AEPD își propune să fie un epicentru pentru idei creative și soluții inovatoare, personalizând principiile existente de protecție a datelor pentru a se potrivi arenei digitale globale. Responsabilitatea este un element-cheie și AEPD încearcă să promoveze

[32] http://www.datepersonale.md/file/Raport/Raport%202016DateENG.pdf
[33] https://edps.europa.eu/press-publications/publications/strategy_en

tehnologii care îmbunătățesc confidențialitatea, transparența, controlul utilizatorilor și răspunderea în prelucrarea datelor importante.
- „Formarea de parteneriate globale”*:* AEPD trebuie să investească în parteneriate globale cu autorități în materie de confidențialitate și protecția datelor, colegi experți, țări din afara UE și organizații internaționale pentru a se ajunge la un consens social privind protecția datelor;
- „Deschiderea unui nou capitol pentru protecția datelor în UE”: AEPD își propune să fie un partener mai proactiv pentru a finaliza un nou cadru juridic al UE privind protecția datelor.

În același timp, Autoritatea Europeană pentru Protecția Datelor stabilește, în fiecare an, prioritățile proprii pentru politica și activitatea consultativă pentru anul următor.

Planul anual se bazează pe programul de lucru al Comisiei Europene, iar Autoritatea Europeană pentru Protecția Datelor adoptă o abordare selectivă, ținând seama, în special, de programul de lucru al Grupul de lucru format în temeiul articolului 29.

8. Comitetul Consultativ al Convenției 108

La nivel internațional, **Comitetul Consultativ al Convenției 108** a identificat următoarele domenii-cheie de intervenție în programul său de lucru pentru perioada 2018-2019[34]:

- urmărirea modernizării Convenției 108;
- promovarea Convenției;
- furnizarea de orientări bazate pe principii la provocările privind viața privată și protecția datelor (genomică și genetică, politici ICANN, inteligență artificială, articularea protecției datelor cu libertatea de exprimare).

[34] https://rm.coe.int/t-pd-2017-wp2018-2019-working-programm-2018-2019-en/168072ab2e

PARTEA 2: ROLUL CONSULTATIV AL AUTORITĂȚII PENTRU PROTECȚIA DATELOR

Autoritățile de protecție a datelor trebuie să promoveze punerea în aplicare a cerințelor privind protecția datelor. Rolul consultativ al autorităților de protecție a datelor este extrem de important pentru îndeplinirea acestui obiectiv.

Articolul 12a din propunerea pentru o Convenție 108 modernizată prevede că **autoritățile de supraveghere sunt consultate cu privire la propunerile privind orice măsuri legislative sau administrative** care prevăd prelucrarea datelor cu caracter personal. În plus, ar trebui să li se solicite autorităților de supraveghere să își dea avizul atunci când se pregătesc alte măsuri privind prelucrarea datelor cu caracter personal, cum ar fi, de exemplu, **codurile de conduită sau normele tehnice**[35].

Operatorii de date trebuie să fie conștienți de obligațiile lor, iar persoanele vizate trebuie să fie informate cu privire la drepturile pe care le au.

Pot fi utilizate diverse instrumente, în funcție de competențele conferite autorităților de protecție a datelor prin legislația națională:

- avize oficiale privind proiectul de lege al parlamentului sau al guvernului care va avea impact asupra protecției datelor sau asupra creării de noi dosare;
- revizuirea notificărilor/autorizațiilor de prelucrare a datelor cu caracter personal;
- răspunsuri la solicitările de consiliere ale operatorilor de date sau ale responsabililor cu protecția datelor;
- dezvoltarea instrumentelor de responsabilitate de către operatorii de date;
- recomandări care să permită autorității de protecție a datelor să-și stabilească „doctrina” în diferite domenii; etc.

În funcție de mandatul dat de legislația națională, autoritatea pentru protecția datelor este, în general, responsabilă de consilierea organizațiilor **private și publice**.

1. Exemple de misiuni consultative ale autorităților de protecție a datelor

1. Georgia

În **Georgia**, rolul consultativ al inspectorului pentru protecția datelor cu caracter personal și al Oficiului său presupune, de exemplu, următoarele funcții:

- **Oferirea de consultări instituțiilor publice și private, precum și persoanelor fizice.** Biroul Inspectorului este deschis pentru consultări pentru a stabili practica corectă a protecției datelor cu caracter personal și pentru a ajuta operatorii de date și persoanele împuternicite de aceștia să respecte reglementările corespunzătoare. De asemenea, Oficiul asistă persoanele în protejarea drepturilor acestora.

[35] http://www.coe.int/en/web/data-protection/modernisation-convention108

- **Elaborarea și emiterea de orientări și recomandări.** Oficiul elaborează orientări și recomandări specifice tematice și sectoriale pentru operatorii de date și persoanele împuternicite de aceștia, pentru a sprijini procesul de punere în practică a dispozițiilor legale.

2. Republica Moldova

În **Moldova**, Centrul Național pentru Protecția Datelor cu Caracter Personal:

- supraveghează respectarea legislației privind protecția datelor cu caracter personal , în special dreptul la informare, acces, corectare, contestare sau eliminare a datelor;
- oferă instrucțiuni necesare pentru ajustarea prelucrării datelor cu caracter personal în conformitate cu principiile legii, fără a afecta domeniul de competență al altor organisme;
- prezintă persoanelor vizate informații cu privire la drepturile acestora legate de prelucrarea datelor cu caracter personal;
- solicită informațiile necesare pentru îndeplinirea sarcinilor sale și primește gratuit aceste informații de la persoane juridice și persoane fizice;
- obține de la deținătorii de date cu caracter personal sprijinul și informațiile necesare pentru îndeplinirea atribuțiilor Centrului[36].

În Raportul său Anual pe 2016, Centrul furnizează detalii privind activitatea sa în acest domeniu. Centrul a emis 84 de avize cu privire la proiecte de reglementări, proiecte de legi și proiecte de versiuni ale tratatelor internaționale privind chestiuni legate de protecția drepturilor și libertăților persoanelor fizice și de prelucrarea datelor cu caracter personal.

Documentele examinate sunt compuse din 15 proiecte de tratate internaționale, 36 de proiecte de regulamente (hotărâri ale Guvernului, decizii ale autorităților publice centrale etc.) și 33 de proiecte de legi (legi și decizii ale Parlamentului).

Centrul reamintește că majoritatea acestor documente au ridicat obiecții care au determinat formularea unor propuneri adecvate, deoarece s-a considerat necesar să se completeze și să se revizuiască textele respective în lumina reglementărilor privind protecția datelor cu caracter personal.

Deoarece unele dintre aceste proiecte prezintă un grad considerabil de intruziune în viața privată, în special slăbirea drepturilor fundamentale ale omului, Centrul a prezentat mai multe recomandări și obiecții pentru a revizui aceste documente în lumina standardelor naționale și europene/ internaționale, unele primind o opinie negativă încă de la început sau ulterior (dacă recomandările și obiecțiile nu au fost luate în considerare de către autori), ca de exemplu:

• Proiectul de lege privind Fondul Arhivistic al Republicii Moldova (propunerile Centrului au fost ignorate în mod repetat de către autori);
• Proiectul de lege privind moratoriul asupra controlului de stat (Centrul nu susține proiectul, considerând că punerea în aplicare a acestei legi ar conduce la un prejudiciu grav atât pentru drepturile persoanelor vizate, cât și pentru drepturile și obligațiile autorităților publice în exercitarea competențelor lor);

[36] http://www.datepersonale.md/md/general/

• Proiectul de lege care modifică și completează legea privind reglementarea valutară (prezentată Centrului fără a lua în considerare propunerile și obiecțiile formulate anterior);
• Proiectul de hotărâre de Guvern cu privire la Sistemul de gestiune a documentelor și înregistrărilor autorităților APC (SIGEDIA), față de care Centrul a formulat obiecții în contextul deficiențelor grave detectate[37].

3. Ucraina

În **Ucraina**, în conformitate cu articolul 23 din Legea Ucrainei privind protecția datelor cu caracter personal, Comisarul are următoarele competențe în domeniul protecției datelor cu caracter personal:

- să primească propuneri, reclamații și alte contestații din partea persoanelor fizice și juridice privind protecția datelor cu caracter personal și să ia decizii în urma examinării lor;
- să aprobe acte normative legale privind protecția datelor cu caracter personal în cazurile prevăzute de Legea privind protecția datelor;
- să ofere recomandări privind aplicarea practică a legislației privind protecția datelor cu caracter personal, să explice drepturile și obligațiile persoanelor relevante la cererea persoanelor vizate, deținătorilor și operatorilor de date cu caracter personal, unităților sau persoanelor responsabile pentru organizarea protecției datelor cu caracter personal, altor persoane;
- să prezinte Președintelui Ucrainei, Cabinetului de Miniștri al Ucrainei, altor organe de stat, organelor autorităților locale autonome și funcționarilor lor, propuneri privind adoptarea sau modificarea actelor normative legale privind protecția datelor cu caracter personal;
- să prezinte concluziile privind proiectele de coduri de conduită în domeniul protecției datelor cu caracter personal și modificările aduse acestora la cererea asociațiilor profesionale, a autorităților autonome locale și a altor asociații publice sau persoane juridice.

[37] http://www.datepersonale.md/file/Raport/Raport%202016DateENG.pdf

2. Avizele autorităților de protecție a datelor cu privire la proiectele de lege și regulamente

Unele autorități pentru protecția datelor au competența de a emite avize formale cu privire la proiectele de legi și conformitatea acestora cu cerințele privind protecția datelor.

Această competență și procedura relevantă sunt detaliate în legislația națională.

Unele autorități au creat proceduri pentru acest rol consultativ.

Exemplu: Metodologia Autorității Europene pentru Protecția Datelor (AEPD) pentru rolul său consultativ

AEPD a emis un document de politică în 2014 cu privire la rolul său consultativ și a propus o nouă legislație[38].

În fiecare an, AEPD publică o listă de priorități pentru politica și activitatea sa consultativă pentru anul următor.

Pentru un maxim de eficiență, AEPD oferă contribuții **într-un stadiu incipient al procesului legislativ.** În conformitate cu o practică bine stabilită, AEPD este consultată de către Comisia Europeană înainte de a adopta o propunere de nouă legislație care ar putea avea un impact asupra dreptului persoanelor la protecția datelor cu caracter personal.

Comentariile informale, care nu sunt publicate, pot fi furnizate într-un stadiu incipient.

Avizele formale se referă la propuneri de legislație și se adresează tuturor celor trei instituții ale UE (Comisie, Consiliu și Parlament) implicate în procesul legislativ, cu scopul de a marca principalele preocupări privind protecția datelor, precum și de a face recomandări. Aceste avize sunt făcute publice și sunt disponibile pe site-ul web al AEPD, precum și în Jurnalul Oficial al UE.

AEPD **monitorizează și noile tehnologii sau alte schimbări în societate** ce pot afecta protecția datelor. Dacă este cazul, Avizul se emite la inițiativa autorității[39].

Se poate spune și că AEPD a dezvoltat un **„Set de instrumente de necesitate”** pentru evaluarea necesității măsurilor care limitează dreptul fundamental la protecția datelor cu caracter personal[40].

[38] https://edps.europa.eu/sites/edp/files/publication/14-06-04_pp_edpsadvisor_en.pdf
[39] https://edps.europa.eu/data-protection/our-role-advisor_en
[40] https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en

3. Rolul privind notificările și autorizațiile

1. Directiva Uniunii Europene 95/46/CE

Articolele 18-20 din **Directiva 95/46/CE a Uniunii Europene** se referă la obligația de notificare a autorității de supraveghere și la verificarea prealabilă a operațiunilor de prelucrare care pot prezenta riscuri specifice pentru drepturile și libertățile persoanei vizate.

Directiva 95/46/CE prevede, de asemenea, că simplificarea sau chiar exceptarea de la notificare poate fi adoptată, de exemplu:

- pentru categoriile de operațiuni de prelucrare care, având în vedere datele care urmează să fie prelucrate, este improbabil să afecteze negativ drepturile și libertățile persoanelor vizate;
- în cazul în care operatorul numește un responsabil de protecție a datelor cu caracter personal;
- pentru prelucrarea al cărei unic scop este păstrarea unui registru care, în conformitate cu legile sau reglementările, are ca scop furnizarea de informații publicului și care este deschis consultării fie de către public în general, fie de orice persoană care demonstrează un interes legitim.

Articolul 19 din Directivă prevede că notificarea trebuie să includă cel puțin:

- numele și adresa operatorului și a reprezentantului său, dacă este cazul;
- scopul sau scopurile prelucrării;
- o descriere a categoriei sau categoriilor de persoane vizate și a datelor sau categoriilor de date referitoare la acestea;
- destinatarii sau categoriile de destinatari cărora le-ar putea fi comunicate datele;
- transferuri propuse de date către țări terțe;
- o descriere generală care să permită o evaluare preliminară a caracterului adecvat al măsurilor luate pentru a asigura securitatea prelucrării.

În final, articolul 20 prevede că statele membre determină operațiunile de prelucrare care pot prezenta riscuri specifice pentru drepturile și libertățile persoanelor vizate și că autoritățile de supraveghere verifică dacă aceste operațiuni de prelucrare sunt examinate înainte de începerea acestora.

2. În unele state membre ale UE

Deoarece practicile de prelucrare a datelor pot fi foarte diverse, statelor sau autorităților le este lăsată o marjă largă de apreciere în privința eventualelor derogări de la această obligație (și orice altă formă de simplificare).

De exemplu, unele state membre ale Uniunii Europene au utilizat în mod extins posibilitatea derogărilor de la obligația de notificare prin creșterea răspunderii operatorului de date - în special prin numirea unui responsabil cu protecția datelor (DPO - Data Protection Officer) - în timp ce altele fac derogări foarte limitate.

În **Franța**, de exemplu, operatorii de date sunt obligați să notifice operațiunile de prelucrare și caracteristicile acestora, cu excepția situațiilor în care sunt scutite de lege sau de autoritatea franceză pentru protecția datelor.

Autoritatea franceză pentru protecția datelor a elaborat un set întreg de norme simplificate, autorizații unice și scutiri care detaliază „doctrina" sa într-un sector specific. De asemenea, se acordă scutiri în cazul în care operatorul a desemnat un responsabil cu protecția datelor[41], cu excepția cazurilor care necesită o autorizație în conformitate cu legea.

De exemplu, Agenția pentru Drepturi Fundamentale a UE reamintește că legislația **Greciei** a introdus inițial un sistem de notificare universală, evitând astfel posibilitatea derogărilor și simplificărilor la procedurile de înregistrare și de notificare oferite de directivă. O modificare ulterioară a legii a introdus posibilitatea derogărilor, ceea ce a dus la o scădere drastică a numărului de notificări[42].

În **Germania**, organismele non-publice au obligația de a notifica operațiunile automatizate de prelucrare a datelor înainte de punerea lor în aplicare, către autoritatea de supraveghere sau comisarul competent pentru protecția datelor. Organele publice ale Federației trebuie să anunțe autoritatea națională cu privire la astfel de operațiuni. Înregistrarea obligatorie nu se aplică dacă operatorul a desemnat un responsabil intern cu protecția datelor. Potrivit Agenției pentru Drepturi Fundamentale, se pare că un număr semnificativ de companii private care sunt obligate prin lege să numească responsabili de protecție a datelor nu respectă această obligație și că acele companii care totuși respectă obligația generală de a desemna responsabili de protecție a datelor foarte des nu facilitează munca eficientă și productivă a celor desemnați[43].

3. De la controlul „ex-ante" al autorității de protecția datelor la controlul „ex-post"

În Uniunea Europeană, având în vedere viitorul RGPD, abordarea generală este să se facă trecerea **de la controlul „ex-ante" al autorității de protecția datelor la controlul „ex-post".** În același timp, RGPD stabilește noi mijloace de prevenire a unor posibile abuzuri.

În ansamblu, obligațiile de notificare și de autorizare vor fi reduse substanțial în cadrul RGPD.

Pe de altă parte, noul Regulament adaugă sau menține anumite obligații de notificare ale autorității de supraveghere, de exemplu în următoarele cazuri:

- notificarea încălcărilor de securitate a datelor fără întârzieri nejustificate și, dacă este posibil, nu mai târziu de 72 de ore de la constatarea acestora, cu excepția cazului în care este puțin probabil ca încălcarea datelor cu caracter personal să ducă la un risc pentru drepturile și libertățile persoanelor fizice (articolul 33);
- în cazul în care o evaluare a impactului privind protecția datelor indică faptul că prelucrarea ar conduce la un risc ridicat în absența măsurilor luate de operator pentru a reduce riscul (articolul 36);

[41] A se vedea, https://www.cnil.fr/fr/deliberations (doar în limba franceză)
[42] http://fra.europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities
[43] http://fra.europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities

- să emită un aviz și să aprobe proiecte de coduri de conduită (articolul 40-5);
- să acrediteze organismele de certificare (articolul 43);
- pentru anumite categorii de transferuri în afara Uniunii Europene (articolele 46-3 și 47); etc.

4. Ucraina

Fiecare autoritate pentru protecția datelor a elaborat propriile formulare de notificare, luând în considerare cerințele naționale.

De exemplu, se poate menționa faptul că autoritatea **ucraineană** pentru protecția datelor a elaborat diverse formulare de notificare.

Un formular este atașat la acest manual în **Anexa 1.**

Și în **Ucraina** a fost aprobat un Ordin specific prin Decretul Comisarului Parlamentului Ucrainei pentru Drepturile Omului la data de 8 ianuarie 2014, nr. 1/ 02-14. Acest Ordin se referă la condițiile de notificare pentru prelucrarea datelor cu caracter personal, care reprezintă un risc deosebit pentru drepturile și libertățile persoanelor vizate.

În special, deținătorul datelor cu caracter personal informează Comisarul cu privire la exercitarea oricărui tip de prelucrare a datelor cu caracter personal, care prezintă un risc deosebit pentru drepturile și libertățile persoanelor vizate, cu excepția cazului în care:

- unicul scop al prelucrării este păstrarea registrului pentru a furniza informații publicului, atunci când acest registru este definit prin lege și este deschis publicului;
- prelucrarea este efectuată de asociații ale societății civile, partide politice și/sau organizații, sindicate, asociații patronale, organizații religioase, organizații ale societății civile de orientare ideologică, cu condiția ca prelucrarea datelor cu caracter personal să privească numai membrii acestor asociații și să nu fie transmise fără consimțământul lor;
- prelucrarea este necesară pentru exercitarea drepturilor și obligațiilor deținătorului de date cu caracter personal în raporturile de muncă, potrivit legii.

5. Georgia

Unele țări au introdus și **un registru public de operatori.** Scopul registrului public este să permită persoanelor să obțină toate informațiile necesare privind operațiunile de prelucrare.

Aceste informații le oferă o imagine de ansamblu asupra utilizării concrete a datelor cu caracter personal și, dacă doresc, își pot exercita drepturile, de exemplu dreptul de acces și dreptul la rectificare.

Acest registru public este, în principiu, accesibil tuturor și nimeni nu trebuie să demonstreze un interes specific pentru a avea acces la el.

În **Georgia**, articolul 19 din Legea privind protecția datelor cu caracter personal obligă operatorii de date să păstreze un catalog de sistem de evidență a datelor pentru fiecare sistem de evidență. Acesta stabilește tipurile de informații care trebuie incluse în catalog și obligă organizațiile de prelucrare a datelor să notifice Oficiul pentru protecția datelor cu caracter personal înainte de a crea un nou sistem de evidență a datelor, adăugând noi categorii de date și/ sau modificând informațiile.

Informațiile incluse în registru sunt publice și inspectorul asigură publicarea acestora conform normelor corespunzătoare. În 2015, Oficiul pentru protecția datelor cu caracter personal a elaborat un registru electronic al cataloagelor sistemelor de evidență. În perioada 2014-2015, Oficiul a digitalizat aproximativ 5 000 de cataloage de sisteme de evidență a datelor furnizate de operatori de date privați sau publici. În plus, inspectorul pentru protecția datelor cu caracter personal a emis în 2016 Ordinul de aprobare a Regulamentului de notificare a inspectorului pentru protecția datelor cu caracter personal privind menținerea cataloagelor sistemelor de evidență a datelor și publicarea cataloagelor sistemelor de evidență a datelor, conform cărora cataloagele sistemelor de evidență pot fi depuse numai în formă electronică prin intermediul registrului electronic al cataloagelor sistemelor de evidență a datelor.

Ordinul a simplificat furnizarea de cataloage de sisteme electronice către Inspectoratul pentru protecția datelor cu caracter personal, precum și actualizarea cataloagelor sistemelor de evidență depuse de operatorii de date. Registrul electronic al cataloagelor sistemelor de evidență permite totodată persoanelor interesate să primească informații despre categoriile de date prelucrate de organizații publice și private[44].

6. Republica Moldova

În **Moldova**, conform prevederilor articolului 23 din Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal, operatorii și persoanele împuternicite de aceștia au obligația de a notifica Centrului operațiunile de prelucrare a datelor cu caracter personal într-un scop specific.

În cursul anului 2016, Departamentul de evidență și control a examinat 850 de notificări pentru înregistrarea operatorilor și a sistemelor automate și/ sau manuale de evidență a datelor cu caracter personal în Registrul de evidență a operatorilor de date cu caracter personal.

Astfel, în această perioadă s-au înregistrat 386 operatori și 761 de sisteme de evidență a datelor cu caracter personal. La examinarea notificărilor de autorizare și de înregistrare prezentate Centrului, în conformitate cu articolul 24 din Legea cu privire la protecția datelor cu caracter personal, au fost efectuate 612 controale prealabile. Mai mult, au fost emise 89 de refuzuri de înregistrare și autorizare a operațiunilor de prelucrare a datelor cu caracter personal.

Din totalul cererilor depuse, în 36 de cazuri au fost autorizate transferuri transfrontaliere de date cu caracter personal, iar în 25 de cazuri acestea au fost refuzate, Centrul indicând considerațiile care au condus la aceste decizii[45].

[44] https://catalog.pdp.ge/
[45] http://www.datepersonale.md/file/Raport/Raport%202016DateENG.pdf

4. Importanța orientărilor și recomandărilor sectoriale

Autoritățile de protecție a datelor trebuie să ofere orientări operatorilor de date, persoanelor împuternicite de către operatori și persoanelor vizate privind punerea în aplicare a unor principii generale de protecție a datelor în sectoare specifice.

În acest sens, una dintre principalele sarcini ale autorităților de protecție a datelor este de a elabora orientări sectoriale care să stabilească „doctrina" autorității de supraveghere.

Ascultarea diferitelor părți interesate cu privire la o chestiune specifică, înainte de a adopta astfel de orientări, poate constitui o bună practică.

1. Armenia

De exemplu, Agenția pentru Protecția Datelor cu Caracter Personal din cadrul Ministerului Justiției al Republicii **Armenia** a publicat un ghid privind protecția datelor cu caracter personal în raporturile de muncă.

Scopul acesteia este asigurarea unui nivel înalt de protecție a datelor cu caracter personal în raporturile de muncă, protejarea drepturilor angajaților (persoanele vizate), informarea angajatorilor (dezvoltatorii de date) cu privire la aspectele principale ale protecției datelor cu caracter personal și asigurarea unei interpretări uniforme a legislației[46].

Autoritatea a publicat, de asemenea, de exemplu, un Ghid privind protecția datelor cu caracter personal ale copiilor.

Scopul Ghidului este să asigure o interpretare integrată a legislației privind protecția datelor cu caracter personal, să crească gradul de conștientizare în rândul copiilor, părinților și operatorilor de date cu privire la drepturile și responsabilitățile acestora și să crească nivelul protecției în ceea ce privește prelucrarea datelor cu caracter personal ale copiilor.

Au fost stabilite principiile protecției copiilor în ceea ce privește prelucrarea datelor cu caracter personal, drepturile copiilor în domeniul protecției datelor cu caracter personal și responsabilitățile operatorilor de date și persoanele împuternicite de aceștia, particularitățile prelucrării datelor cu caracter personal în cadrul instituțiilor de învățământ, pe internet și în mass-media și răspunderea preconizată pentru încălcarea dreptului la protecția datelor cu caracter personal ale copiilor[47].

2. Georgia

Autoritatea pentru protecția datelor din **Georgia** a publicat pe site-ul său web următoarele orientări, disponibile în limba engleză:

- recomandări privind prelucrarea datelor biometrice;
- recomandări pentru realizarea supravegherii video;

[46] http://www.moj.am/en/article/1760
[47] http://www.moj.am/en/article/1718

- recomandări privind prelucrarea datelor cu caracter personal în scopuri de marketing direct;
- recomandări privind protecția datelor cu caracter personal în raporturile de muncă[48].

Inspectorul a publicat (actualmente doar în limba georgiană) și recomandări privind prelucrarea datelor referitoare la sănătate, recomandări pentru școli și pentru părinții elevilor, recomandări pentru furnizorii și utilizatorii de servicii de internet etc.

3. Republica Moldova

Centrul Național pentru Protecția Datelor al Republicii **Moldova** a emis, de asemenea, mai multe recomandări cu privire la aspecte specifice. De exemplu, se pot menționa următoarele instrucțiuni, disponibile în limba engleză pe site-ul instituției:
- Instrucțiuni privind prelucrarea datelor cu caracter personal în procesul electoral.
- Instrucțiuni privind prelucrarea datelor cu caracter personal în sectorul de poliție
- Instrucțiuni privind prelucrarea datelor cu caracter personal în sectorul educației [49].

De asemenea, acesta a emis mai multe recomandări și videoclipuri privind protecția datelor cu caracter personal ale copiilor[50].

Prin viitorul proiect Twinning finanțat de UE, sunt planificate mai multe orientări și recomandări în următoarele sectoare: financiar-bancar; IT și comunicații electronice; mass-media; sănătate; polițienesc și supraveghere video, iar unele dintre cele existente vor fi revizuite, ca de exemplu cea referitoare la procesul electoral.

4.

În general, ar trebui să se facă trimitere și la numeroasele avize, recomandări, rezoluții și orientări elaborate de:
- Comitetul Consultativ al Convenției 108[51];
- Grupul de lucru în temeiul articolului 29 al Uniunii Europene (aproape 250 de avize)[52;]
- Conferința Internațională a Comisarilor pentru Protecția Datelor și a Vieții Private[53];
- toate autoritățile de protecție a datelor de la nivel național[54].

Acest set extins de instrumente disponibile publicului poate oferi orientări pentru alte autorități de supraveghere, dar și pentru operatori, persoanele împuternicite de operatori sau persoane fizice.

[48] https://personaldata.ge/en/publications/recommendations
[49] http://www.datepersonale.md/md/decizii/instructiuni/
[50] http://www.datepersonale.md/md/copii-protectie/
[51] http://www.coe.int/en/web/data-protection/reports-studies-and-opinions
[52] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 ;
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm
[53] https://icdppc.org/document-archive/
[54] http://ec.europa.eu/justice/data-protection/bodies/index_en.htm

5. Rolul tot mai mare al responsabilității și responsabilii de protecția datelor

1. Există o tendință crescătoare de trecere de la o supraveghere *ex-ante* la o supraveghere *ex-post.*

În cazul în care sistemul de reglementare a protecției datelor era, în unele țări, anterior în mare parte bazat pe notificări și autorizații, există o creștere evidentă a dezvoltării principiului responsabilității.

RGPD integrează responsabilitatea ca principiu care impune ca organizațiile să pună în aplicare măsuri tehnice și organizatorice adecvate și să poată demonstra, la cerere, ce au făcut și eficacitatea acțiunilor lor.

Ideea generală este să se integreze o „cultură a protecției datelor" în cadrul organizațiilor care prelucrează date cu caracter personal.

În acest sens, ar trebui dezvoltate instrumente care să demonstreze această conformitate. În unele cazuri, anumite instrumente sunt obligatorii și trebuie implementate de operatori.

În orice caz, chiar dacă nu există nicio obligație legală, dezvoltarea de programe și instrumente de către operatorii de date sau persoanele împuternicite de aceștia poate fi încurajată de autoritățile de protecție a datelor.

Obiectivul este să se dezvolte un „set de instrumente" de conformitate prin utilizarea diferitelor mijloace de acțiune: documentația adecvată privind prelucrarea datelor cu caracter personal, în ce mod, în ce scop, cât timp; procese și proceduri documentate care vizează abordarea problemelor legate de protecția datelor din timp atunci când se construiesc sisteme de informare sau se răspunde la o încălcare a securității datelor; responsabilii de protecție a datelor care formează o rețea privilegiată de experți; dezvoltarea de certificări și, de exemplu, reguli corporative obligatorii care reglementează transferurile de date cu caracter personal în cadrul companiilor multinaționale; crearea de „pachete de conformitate" de către autoritatea de protecția datelor, care sunt modele de referință bazate pe sectoare, care acoperă un întreg sector sau o ramură profesională; etc

2. Responsabilii cu protecția datelor

Într-o abordare bazată pe responsabilitate, **responsabilii cu protecția datelor** se află în centrul cadrului juridic și ar trebui să faciliteze respectarea cerințelor privind protecția datelor.

În acest sens, responsabilii pentru protecția datelor au devenit actori absolut esențiali în cadrul organizațiilor publice și private care se ocupă de datele cu caracter personal.
În conformitate cu RGPD, este obligatoriu ca anumiți operatori și persoanele împuternicite de aceștia să desemneze un responsabil cu protecția datelor (DPO – Data protection officer).

Acest lucru este valabil pentru toate autoritățile și organismele publice (indiferent de datele pe care le prelucrează) și pentru alte organizații care - ca activitate de bază - monitorizează persoanele în mod sistematic și la scară largă sau care prelucrează categorii speciale de date cu caracter personal pe scară largă.

Grupul de lucru în temeiul articolului 29 a adoptat deja Orientări privind responsabilii cu protecția datelor.

În particular, Grupul de lucru în temeiul articolului 29 prevede că: „DPO este piatra de temelie a responsabilității și numirea unui DPO poate facilita conformitatea și, în plus, poate deveni un avantaj competitiv pentru întreprinderi. Pe lângă facilitarea conformității prin implementarea unor instrumente de responsabilitate (cum ar fi facilitarea sau realizarea evaluărilor de impact privind protecția datelor și a auditurilor), DPO acționează ca intermediar între părțile interesate relevante (de exemplu, autoritățile de supraveghere, persoanele vizate și unitățile de lucru din cadrul unei organizații).

DPO nu sunt responsabili personal în cazul nerespectării RGPD. RGPD clarifică faptul că operatorul sau persoana împuternicită de acesta trebuie să se asigure și să demonstreze că prelucrarea este efectuată în conformitate cu dispozițiile sale [articolul 24 alineatul (1)].

Conformitatea cu protecția datelor este responsabilitatea operatorului sau a persoanei împuternicite de acesta. Operatorul sau persoana împuternicită joacă, de asemenea, un rol esențial în a permite îndeplinirea eficientă a sarcinilor DPO. Numirea unui DPO este un prim pas, însă DPO-ului trebuie să i se acorde suficientă autonomie și resurse pentru a-și îndeplini sarcinile în mod eficient.”[55].
Totodată, trebuie încurajată formarea DPO și înființarea de rețele de DPO.

3. Evaluările impactului asupra vieții private

În plus, **evaluările impactului asupra vieții private** vor juca un rol din ce în ce mai important în promovarea conformității.
Articolul 35 din RGPD introduce în dreptul UE conceptul de evaluare a impactului protecției datelor (DPIA - Data Protection Impact Assessment).

DPIA este un proces destinat să descrie prelucrarea, să evalueze legitimitatea și temeiul juridic al fiecărui scop, necesitatea și proporționalitatea unei prelucrări în ceea ce privește datele prelucrate și să ajute la gestionarea riscurilor pentru drepturile și libertățile persoanelor fizice care sunt asociate prelucrării datelor cu caracter personal (prin evaluarea acestora și prin stabilirea măsurilor de abordare a riscurilor).

Evaluările DPIA sunt instrumente importante pentru responsabilizare, deoarece acestea ajută operatorii nu doar să respecte cerințele RGPD, ci și să demonstreze că au fost luate măsurile adecvate pentru a se asigura conformitatea.

Ținând seama de abordarea bazată pe risc, implementată de RGPD, efectuarea DPIA nu este obligatorie pentru fiecare operațiune de prelucrare. O DPIA este necesară numai atunci când prelucrarea este „susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice”.
Pe această temă, Grupul de lucru în temeiul articolului 29 a elaborat deja orientări specifice[56].

[55] http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf
[56] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

4. Certificările

Unele autorități de protecție a datelor au tot mai multă putere de emitere a **certificărilor** pentru produse sau proceduri care tratează chestiunea protecției datelor.

De obicei, certificarea permite unui operator să se distingă de ceilalți prin calitatea serviciilor oferite. Pentru utilizatori, este un indicator de încredere privind produsele, serviciile și procedurile TIC, care permite utilizatorilor să identifice și să favorizeze organizațiile care garantează un nivel ridicat de protecție a datelor cu caracter personal.

În cele din urmă, RGPD încurajează elaborarea de **coduri de conduită** care să fie aprobate de autoritatea pentru protecția datelor. Aceste coduri de conduită intenționează să contribuie la aplicarea corectă a RGPD, ținând cont de particularitățile diferitelor sectoare de prelucrare și de nevoile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii.

Aceste coduri de conduită pot fi elaborate de asociații și alte organisme care reprezintă categorii de operatori sau persoane împuternicite de aceștia sau categorii de persoane vizate. Acestea ar trebui să conțină mecanisme eficiente de monitorizare a respectării dispozițiilor de către operatorii sau persoanele împuternicite de aceștia, care se angajează să o aplice. Aceste mecanisme nu împiedică persoanele vizate să se adreseze autorității de protecție a datelor sau autorităților judiciare.

6. Inovare și cercetare

De asemenea, autoritățile de protecție a datelor ar trebui încurajate să stabilească cât mai curând posibil relații ferme cu **experții în cercetare și inovare** la nivel înalt, cu industria și serviciile IT, cu autoritățile publice, cu reprezentanți ai sectorului privat și ai ONG-urilor.

Autoritățile de supraveghere trebuie să fie pe deplin conștiente de noile evoluții tehnologice și să însoțească aceste evoluții cât mai curând posibil.

1. Exemplu francez

De exemplu, autoritatea franceză pentru protecția datelor, CNIL, dispune de un **laborator** la sediul său, care este dedicat testării și experimentării produselor și aplicațiilor de vârf. Acest laborator testează produsele, aplicațiile și serviciile în etapa beta, pentru a evalua impactul lor potențial asupra vieții private a persoanelor vizate. Având în vedere principiul „confidențialității prin proiectare”, CNIL se străduiește să integreze cerințele de protecție a datelor în cadrul arhitecturilor tehnologice, dezvoltărilor IT și noilor servicii.

Pentru a-și consolida misiunea de elaborare și reflectare asupra potențialelor perspective, CNIL a înființat în 2012 un **Comitet prospectiv** care reunește experți externi. Se urmărește consolidarea a două obiective: luarea în considerare, într-un stadiu foarte timpuriu, a unor subiecte noi precum tendințele, tehnologiile sau utilizările viitoare pentru date și evaluarea studiilor de caz și a analizelor efectuate cu ajutorul unor instrumente și proiecte inovatoare.

În cele din urmă, CNIL a creat și un **premiu** în domeniul protecției datelor, recunoscând valoarea operelor academice și încurajând dezvoltarea cercetării privind protecția datelor și drepturile de confidențialitate în universități. Acest premiu acoperă multe discipline diferite, precum: științe sociale, drept, științe politice, economie, dar și domenii tehnice[57].

2. Autoritatea Europeană pentru Protecția Datelor

Pentru a da un alt exemplu, Autoritatea Europeană pentru Protecția Datelor (AEPD) a identificat marile volume de date (Big Data) și extragerea datelor (Data Mining) ca o posibilă amenințare atât la adresa dreptului la viață privată și a protecției datelor, cât și a altor drepturi fundamentale, inclusiv libertatea de exprimare și nediscriminarea.

Volumele mari de date reprezintă o preocupare strategică pe termen lung pentru autoritățile de protecție a datelor, dar și pentru alte agenții de aplicare a legii în domeniul concurenței și al protecției consumatorilor.

Având în vedere acest lucru, AEPD a propus crearea unui mecanism **„clearing house" digital** care reunește agențiile din domeniile concurenței, protecției consumatorilor și datelor care doresc să facă schimb de informații și să discute despre cele mai bune modalități de punere în aplicare a normelor în interesul persoanei.

Prin această inițiativă, AEPD intenționează să încurajeze o dezbatere la nivel mondial cu privire la implicațiile volumelor mari de date și la necesitatea ca legiuitorii și autoritățile de reglementare să reflecte asupra problemei[58].

[57] https://www.cnil.fr/en/cnils-missions
[58] https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en

PARTEA 3: ROLUL DE SUPRAVEGHERE AL AUTORITĂȚILOR PENTRU PROTECȚIA DATELOR

Autoritățile de protecție a datelor au competența de a monitoriza respectarea legislațiilor privind protecția datelor.

În acest scop, autoritățile de protecție a datelor dețin, de regulă, competențe de supraveghere „ex-post" care le permit să primească și să gestioneze reclamațiile persoanelor, să efectueze inspecții la operatorii de date și la persoanele împuternicite de aceștia, să adopte sancțiuni și/ sau să trimită cazuri autorităților judiciare.

1. Tratarea reclamațiilor

1. Standarde internaționale

Articolul 1 din Protocolul adițional la Convenția 108 prevede că autoritățile de supraveghere „au, în special, competențe de investigare și intervenție, precum și competența de a se angaja în proceduri judiciare sau de a aduce la cunoștința autorităților judiciare competente încălcări ale dispozițiilor interne prin care se aplică principiile menționate la articolul 1 alineatul (1) din prezentul Protocol.

Fiecare autoritate de supraveghere audiază cererile depuse de orice persoană cu privire la protecția drepturilor și a libertăților fundamentale ale acesteia în ceea ce privește prelucrarea datelor cu caracter personal de competența sa".

Articolul 12a al textului consolidat al propunerilor de modernizare la Convenția 108 finalizate de CAHDATA (reuniunea din 15-16 iunie 2016[59]) prevede, de asemenea, că „fiecare autoritate de supraveghere competentă se ocupă de cererile și reclamațiile depuse de persoanele vizate cu privire la drepturile lor de protecție a datelor și informează persoanele vizate asupra progresului".

În conformitate cu articolul 57 din RGPD, fiecare autoritate de supraveghere tratează reclamațiile depuse de o persoană vizată sau de un organism, organizație sau asociație și investighează, în măsura în care este cazul, obiectul reclamației și informează reclamantul cu privire la progresul și rezultatele investigației într-o perioadă rezonabilă, în special dacă este necesară o anchetă sau o coordonare suplimentară cu o altă autoritate de supraveghere.

Fiecare autoritate de supraveghere facilitează depunerea reclamațiilor prin măsuri precum un formular de depunere a reclamației, care poate fi completat și electronic, fără a exclude alte mijloace de comunicare.

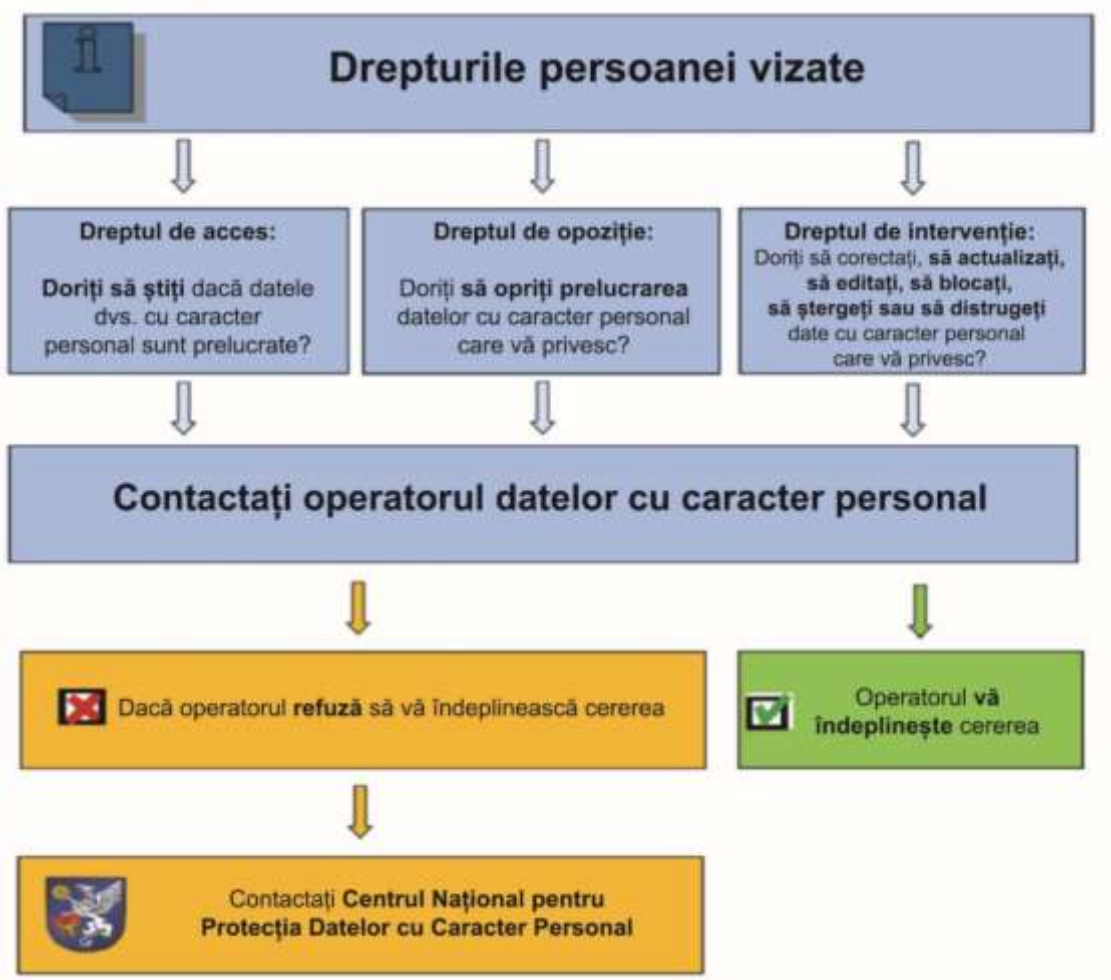
Executarea sarcinilor fiecărei autorități de supraveghere este gratuită pentru persoana vizată și, după caz, pentru responsabilul cu protecția datelor.

[59] Cf. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a616c

Posibilitatea ca persoanele să depună o reclamație este un element-cheie pentru o arhitectură eficientă care să permită protecția persoanei în ceea ce privește prelucrarea datelor cu caracter personal. Aceasta ajută la garantarea dreptului la un remediu adecvat. Reclamațiile pot fi depuse, de exemplu, dacă se colectează cantități excesive de date cu caracter personal; în cazul în care o persoană nu este lăsată să-și acceseze propriile date personale; dacă datele au fost prelucrate ilegal; etc.

2. Republica Moldova

În Moldova, Centrul Național pentru Protecția Datelor cu Caracter Personal a emis, în raportul său anual pentru anul 2016, o descriere a procedurii de exercitare a drepturilor persoanelor vizate:



Numărul reclamațiilor primite este un indicator important al nivelului de cunoaștere de către persoane a drepturilor pe care le au, astfel cum este evidențiat de autoritatea de protecție a datelor în raportul său anual[60].

[60] http://www.datepersonale.md/file/Raport/Raport%202016DateENG.pdf

Evoluția numărului de plângeri depuse la Centrul Național pentru Protecția Datelor cu Caracter Personal din Republica Moldova în perioada 2009-2016

Creșterea considerabilă a numărului de reclamații primite în cursul anului 2015 (cu 37 % față de 2014) demonstrează că persoanele vizate au înțeles mai bine, în comparație cu anii anteriori, atribuțiile CNPDCP și au mai multă încredere în eficiența acțiunilor întreprinse de autoritatea națională de supraveghere pentru protecția datelor cu caracter personal în apărarea drepturilor și libertăților lor fundamentale.

Reclamațiile primite de către CNPDCP au vizat o gamă largă de aspecte legate de prelucrarea datelor cu caracter personal în sectorul financiar-bancar, sectorul sănătății, servicii publice, supravegherea video a spațiilor publice și/ sau private, condițiile de prelucrare a datelor cu caracter personal pentru operatori și destinatari, aspectele legate de divulgarea datelor cu caracter personal și nerespectarea măsurilor de securitate și confidențialitate.

În 2016, în 171 de cazuri, CNPDCP a inițiat controale de legalitate privind prelucrarea datelor cu caracter personal pe baza reclamațiilor. În 113 cazuri, persoanele vizate au contactat CNPDCP pentru a semnala încălcarea dispozițiilor legale referitoare la condițiile în care datele cu caracter personal au fost divulgate unor terți fără obținerea consimțământului prealabil al persoanelor vizate sau fără a lua suficient în considerare dreptul la informare al respectivei persoane, prelucrarea datelor cu caracter personal fără temei juridic sau disproporționat în raport cu scopul urmărit, divulgarea datelor cu caracter personal într-o manieră nerestricționată pe internet sau pe site-urile mass-media ori pe site-urile și blogurile unei companii sau prin utilizarea rețelelor de partajare a fișierelor.

În 2015, s-ar putea observa o creștere semnificativă a documentelor primite de la persoane juridice de drept public și privat. În special, un procent semnificativ din aceste documente provin de la instituții precum Ministerul Afacerilor Interne, Ministerul Sănătății, Ministerul Tehnologiei Informației și Comunicațiilor, Ministerul Justiției, Cancelaria de Stat, dar și de la părțile interesate din sectorul financiar-bancar, turism, comerț, domeniul sferei de servicii - entități implicate direct în prelucrarea datelor cu caracter personal.

3. Georgia

În **Georgia**, Oficiul examinează legalitatea prelucrării datelor în instituțiile publice și private. Inspectorul este împuternicit să verifice operatorii de date și persoanele împuternicite de aceștia pe baza cererilor primite și din oficiu. Inspectorul este autorizat să acceseze orice informații de la operatorii de date, inclusiv informații considerate secret de stat, comercial sau profesional.

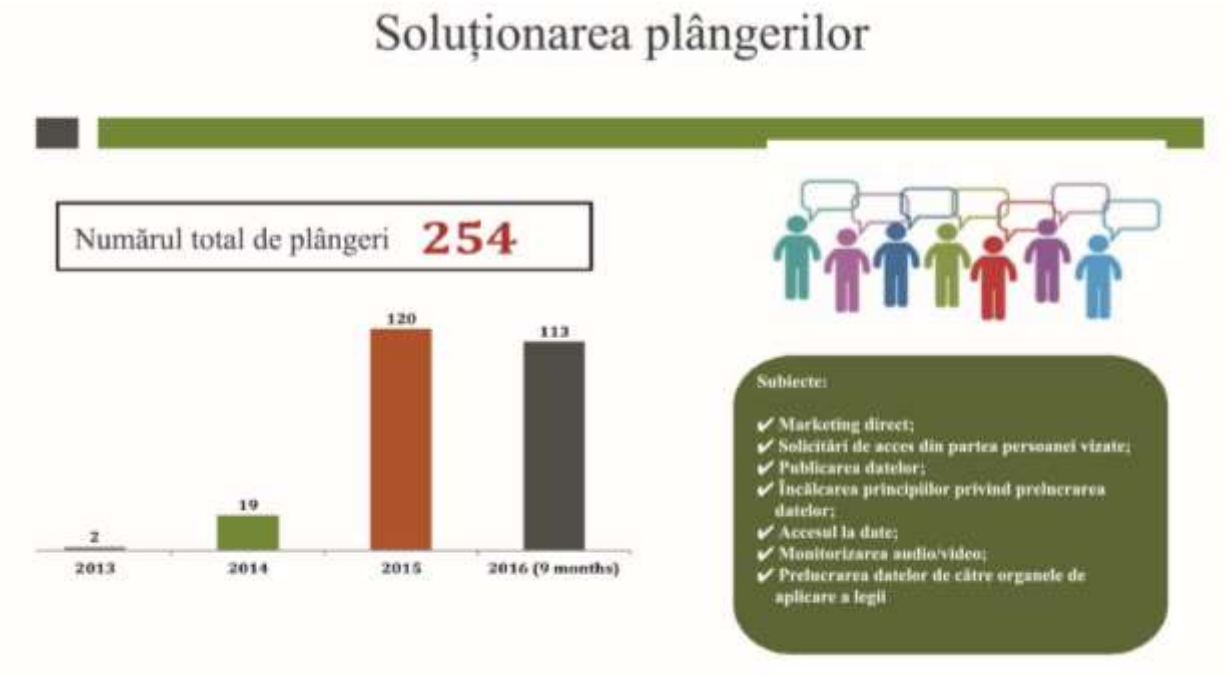
Acesta se ocupă de reclamațiile persoanelor fizice și este autorizat să ia măsurile prevăzute de lege. În timpul examinării reclamației, inspectorul analizează datele și circumstanțele. Dacă este necesar, inspectorul solicită informații suplimentare și verifică operatorul de date și/sau persoana împuternicită de acesta. Termenul pentru soluționarea reclamațiilor este de două luni. Acest termen poate fi prelungit pentru o perioadă de o lună, prin decizia motivată a inspectorului.

În cazul în care se constată prelucrarea ilegală a datelor, inspectorul are dreptul:

- de a cere eliminarea încălcărilor și a discrepanțelor aferente în termenul solicitat și în modul recomandat;
- de a cere încetarea temporară sau permanentă a prelucrării datelor;
- de a cere obstrucționarea, ștergerea, distrugerea și/ sau depersonalizarea datelor;
- de a cere încetarea fluxului transfrontalier de date;
- de a furniza recomandări operatorului de date și/ sau persoanei împuternicite de acesta în cazul unor încălcări minore;
- de a se adresa instanțelor în cazul în care operatorul de date sau persoana împuternicită de acesta nu îndeplinește cererea inspectorului;
- de a elabora un proces verbal în cazul în care se constată o contravenție și se impune responsabilitatea administrativă a operatorului de date/ persoanei împuternicite de acesta;
- de a se adresa organelor de drept în cazul în care se constată elementele unei infracțiuni.

În Georgia, în 2016[61], numărul consultărilor acordate persoanelor fizice, organizațiilor publice și private a crescut de trei ori; numărul reclamațiilor și inspecțiilor a crescut de două ori; au fost constatate 221 fapte de încălcare; 63 de organizații au fost sancționate cu amendă, în timp ce 35 de organizații au primit avertisment[62].

[61] https://personaldata.ge/manage/res/images/2017/angarishi/2016%20Eng.pdf
[62] https://rm.coe.int/16806eead9



4. Ucraina

În **Ucraina**, pe site-ul oficial al Comisarului pentru drepturile omului al Parlamentului ucrainean, se pot găsi informații despre modul de depunere a reclamațiilor în atenția Comisarului.

Reclamațiile adresate Comisarului Parlamentului ucrainean pentru drepturile omului sunt prezentate în scris și pot fi trimise și prin e-mail. Acestea vor menționa diverse informații, inclusiv detalii despre reclamant și fondul cererii.

Cetățenii ucraineni, indiferent de locul lor de ședere temporară, străinii și apatrizii care locuiesc pe teritoriul Ucrainei sau persoanele care acționează în numele lor pot depune o reclamație în termen de un an de la divulgarea actelor de încălcare a drepturilor și libertăților omului. În cazuri excepționale, această perioadă poate fi prelungită de Comisar, dar nu ar trebui să depășească doi ani[63].

Comisarul furnizează și informații extensive privind criteriile de inadmisibilitate[64].

638 de reclamații au fost depuse în 2015 în materie de protecția datelor și 1 306 de reclamații în 2016[65].

Reclamațiile se referă de obicei la transferurile de date cu caracter personal către terți; motivele legale pentru prelucrarea datelor cu caracter personal; accesul persoanei vizate la datele sale personale; respectarea legislației privind protecția datelor cu caracter personal pe internet.

[63] http://www.ombudsman.gov.ua/en/page/applicant/admissibility-criteria-for-petitions-to-the-commissioner/
[64] http://www.ombudsman.gov.ua/en/page/applicant/inadmissible-petitions/
[65] https://rm.coe.int/16806eeae1

5. Regatul Unit

Autoritatea de supraveghere poate, de asemenea, să furnizeze, ca o bună practică, modele de scrisori pentru persoane fizice, de exemplu, pentru a avea acces la datele lor personale sau pentru a contesta acțiunile operatorilor sau a persoanelor împuternicite de aceștia.

De exemplu, Biroul Comisarului pentru Informații din Regatul Unit publică astfel de modele pe site-ul său web[66].

Biroul Comisarului pentru Informații publică, de asemenea, o listă de cazuri concrete, care descriu metodologia utilizată în soluționarea unui caz[67].

În Anexă sunt prezentate câteva exemple.

6. Uniunea Europeană

Pentru **Uniunea Europeană**, AEPD oferă consiliere cu privire la modul în care persoanele își pot exercita drepturile sau pot depune o reclamație.

Persoanele care consideră că drepturile le-au fost încălcate pot completa un formular de reclamație online[68].

În principiu, operatorul sau responsabilul cu protecția datelor trebuie să fie contactat înainte de adresarea unei reclamații către AEPD.

Reclamația trebuie făcută în termen de doi ani de la data la care persoana constată faptele pe care se bazează reclamația sa.

AEPD gestionează reclamația în regim confidențial. Cu toate acestea, instituția în cauză poate fi informată în legătură cu investigația. Petiționarul poate depune o cerere de a rămâne anonim. Dacă această solicitare nu este îndeplinită, persoana poate decide să retragă sau să meargă mai departe cu reclamația.

Pentru a investiga o reclamație, AEPD are dreptul să obțină toate datele cu caracter personal și toate informațiile necesare pentru anchetele din partea instituției UE în cauză. De asemenea, poate avea acces la sediile oricărei instituții UE în cazul în care este necesară o investigație la fața locului. Reclamațiile pot fi soluționate și din inițiativa inspectorului.

[66] https://ico.org.uk/for-the-public/raising-concerns/
[67] https://ico.org.uk/action-weve-taken/case-stories/case-story-10/
[68] https://edps.europa.eu/node/75

7. Franța

În Franța, CNIL oferă pe site-ul său un serviciu online de reclamații, cum ar fi: ștergerea datelor cu caracter personal de pe internet, obiecția cu privire la primirea de publicitate prin poștă și actualizarea corectitudinii datelor cu caracter personal[69].

Soluția, în unele cazuri, poate fi găsită printr-o simplă mediere informală operată la inițiativa CNIL împreună cu operatorul.

În numele persoanelor vizate, CNIL poate accesa dosare de securitate națională, de apărare și de securitate publică care conțin datele lor - în special certificatele de cazier judiciar și dosarele de supraveghere. Acest tip de acces se numește **acces indirect.** Atunci când solicită CNIL să consulte aceste fișiere, persoana trebuie să facă o adresă către CNIL, indicând exact adresa și numărul său de telefon și atașând și o fotocopie a cărții de identitate.

2. Procedura de desfășurare a inspecțiilor

1. Standarde europene

În conformitate cu Protocolul adițional la Convenția 108 și cu textul modernizat propus, autoritățile de supraveghere au competențe de investigare și de intervenție.

Autoritățile de protecție a datelor au, în special, posibilitatea de a solicita operatorului și persoanei autorizate de acesta informații privind prelucrarea datelor cu caracter personal și de a le obține.

Conform proiectului de raport explicativ la propunerile de modernizare, puterea de intervenție a autorității de supraveghere „*poate lua diverse forme în legislația Părții. De exemplu, autoritatea ar putea fi împuternicită să oblige operatorul să rectifice, să șteargă sau să distrugă datele incorecte sau prelucrate în mod ilegal în cont propriu sau în cazul în care persoana vizată nu este în măsură să exercite personal aceste drepturi.*

Puterea de a lua măsuri împotriva operatorilor care nu doresc să comunice informațiile solicitate într-un termen rezonabil ar fi, de asemenea, o demonstrație deosebit de eficientă a puterii de intervenție”[70].

În baza RGPD, fiecare autoritate de supraveghere monitorizează și pune în aplicare legea. Aceasta efectuează investigații privind aplicarea regulamentului, inclusiv pe baza informațiilor primite de la o altă autoritate de supraveghere sau de la o altă autoritate publică.

În conformitate cu articolul 58 din RGPD, „Fiecare autoritate de supraveghere are toate următoarele competențe de investigare:
(a) de a da dispoziții operatorului și persoanei împuternicite de operator și, după caz,

[69] https://www.cnil.fr/fr/plaintes
[70] https://rm.coe.int/16806b6ec2

reprezentantului operatorului sau al persoanei împuternicite de operator să furnizeze orice informații pe care autoritatea de supraveghere le solicită în vederea îndeplinirii sarcinilor sale;

(b) de a efectua investigații sub formă de audituri privind protecția datelor;

(c) de a efectua o revizuire a certificărilor acordate în temeiul articolului 42 alineatul (7);

(d) de a notifica operatorul sau persoana împuternicită de operator cu privire la presupusa încălcare a prezentului regulament;

(e) de a obține, din partea operatorului și a persoanei împuternicite de operator, accesul la toate datele cu caracter personal și la toate informațiile necesare pentru îndeplinirea sarcinilor sale;

(f) de a obține accesul la oricare dintre incintele operatorului și ale persoanei împuternicite de operator, inclusiv la orice echipamente și mijloace de prelucrare a datelor, în conformitate cu dreptul Uniunii sau cu dreptul procesual intern.

2. Fiecare autoritate de supraveghere are toate următoarele competențe corective:

(a) de a emite avertizări în atenția unui operator sau a unei persoane împuternicite de operator cu privire la posibilitatea ca operațiunile de prelucrare prevăzute să încalce dispozițiile prezentului regulament;

(b) de a emite mustrări adresate unui operator sau unei persoane împuternicite de operator în cazul în care operațiunile de prelucrare au încălcat dispozițiile prezentului regulament;

(c) de a da dispoziții operatorului sau persoanei împuternicite de operator să respecte cererile persoanei vizate de a-și exercita drepturile în temeiul prezentului regulament;

(d) de a da dispoziții operatorului sau persoanei împuternicite de operator să asigure conformitatea operațiunilor de prelucrare cu dispozițiile prezentului regulament, specificând, după caz, modalitatea și termenul-limită pentru aceasta;

(e) de a obliga operatorul să informeze persoana vizată cu privire la o încălcare a protecției datelor cu caracter personal;

(f) de a impune o limitare temporară sau definitivă, inclusiv o interdicție asupra prelucrării;

(g) de a dispune rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării, în temeiul articolelor 16, 17 și 18, precum și notificarea acestor acțiuni destinatarilor cărora le-au fost divulgate datele cu caracter personal, în conformitate cu articolul 17 alineatul (2) și cu articolul 19;

(h) de a retrage o certificare sau de a obliga organismul de certificare să retragă o certificare eliberată în temeiul articolul 42 și 43 sau de a obliga organismul de certificare să nu elibereze o certificare în cazul în care cerințele de certificare nu sunt sau nu mai sunt îndeplinite;

(i) de a impune amenzi administrative în conformitate cu articolul 83, în completarea sau în locul măsurilor menționate la prezentul alineat, în funcție de circumstanțele fiecărui caz în parte;

(j) de a dispune suspendarea fluxurilor de date către un destinatar dintr-o țară terță sau către o organizație internațională.[71] *"*

[71] http://eur-lex.europa.eu/legal-content/EN-RO/TXT/?uri=CELEX:32016R0679&from=EN

2. Republica Moldova

În **Moldova**, controlul conformității operațiunilor de prelucrare a datelor cu caracter personal se efectuează exclusiv de către Centrul Național pentru Protecția Datelor cu Caracter Personal, cu excepția cazurilor prevăzute la articolul 2 alineatul (4) din Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal.

Controlul legalității prelucrării datelor cu caracter personal poate fi inițiat pe baza reclamației persoanei vizate, prin notificare/din oficiu sau în contextul cererilor de autorizare a transferurilor transfrontaliere.

Articolul 74 din Codul Contravențional al Republicii Moldova prevede că, în cazul în care persoana verificată refuză să permită accesul Centrului Național pentru Protecția Datelor cu Caracter Personal la informații, se poate impune o amendă de la 100 la 500 de euro.

În 2016, a fost înregistrată o creștere semnificativă a numărului total de controale inițiate pe baza reclamațiilor persoanelor vizate. În același timp, s-a înregistrat o scădere substanțială a numărului de controale inițiate în privința transferurilor de date personale transfrontaliere. Prin urmare, în această perioadă au fost inițiate și examinate **247** de controale, dintre care **186** au fost inițiate pe baza reclamațiilor persoanelor vizate, prin sesizare/ din oficiu, și **61** pe baza cererilor de autorizare a transferurilor transfrontaliere.

În 2016, **au avut loc acțiuni de control al legalității prelucrării din oficiu**, în urma procedurii scrise de obținere a informațiile necesare pentru examinarea circumstanțelor invocate și stabilirea unei soluții. În acest context, trebuie menționat faptul că, pentru a clarifica circumstanțele și a examina în mod obiectiv cazurile investigate de CNPDCP, angajații săi, în majoritatea cazurilor, trebuiau să se deplaseze la fața locului. Cu toate acestea, având în vedere numărul redus de angajați și activitățile multiple care se suprapun în această perioadă, în majoritatea cazurilor, dovezile au fost colectate ca urmare a trimiterii de cereri/solicitări. Angajații CNPDCP sunt, prin urmare, obligați să utilizeze informațiile declarate fără a putea verifica veridicitatea acestora. Această situație poate fi depășită prin creșterea substanțială a numărului de angajați ai subdiviziunii competente a Centrului[72].

[72] http://www.datepersonale.md/file/Raport/Raport%202016DateENG.pdf

Date comparative ale activității de control desfășurate de către Centru în perioada 2014-2016

	Controale inițiate în temeiul:		actelor emise ca răspuns la controale			
Perioada de comparație	Plângeri/ sesizări	Solicitări de transfer transfrontalier	Decizii privind suspendarea prelucrării datelor cu caracter personal	Decizii privind încetarea prelucrării datelor cu caracter personal	Decizie privind distrugerea/ștergerea datelor cu caracter personal prelucrate cu încălcarea legii	Cazuri de contravenții fondate/procese-verbale emise
2014	140	34	1	3	1	56/34
2015	149	469	4	8	-	43/24
2016	186	61	18	11	2	66/33

3. Georgia

În **Georgia**, Inspectorul pentru protecția datelor cu caracter personal verifică legalitatea procesării datelor din proprie inițiativă sau pe baza unei reclamații.

Inspecția implică:

- stabilirea existenței temeiurilor și principiilor prelucrării legitime a datelor;
- examinarea conformității măsurilor de securitate organizațională și tehnică a datelor cu cerințele legislației;
- examinarea conformității sistemului de evidență a datelor, a catalogului sistemului de evidență și a înregistrărilor privind divulgarea datelor cu caracter personal cu cerințele legale stabilite;
- examinarea legitimității fluxului transfrontalier de date;
- examinarea respectării altor cerințe ale legislației.

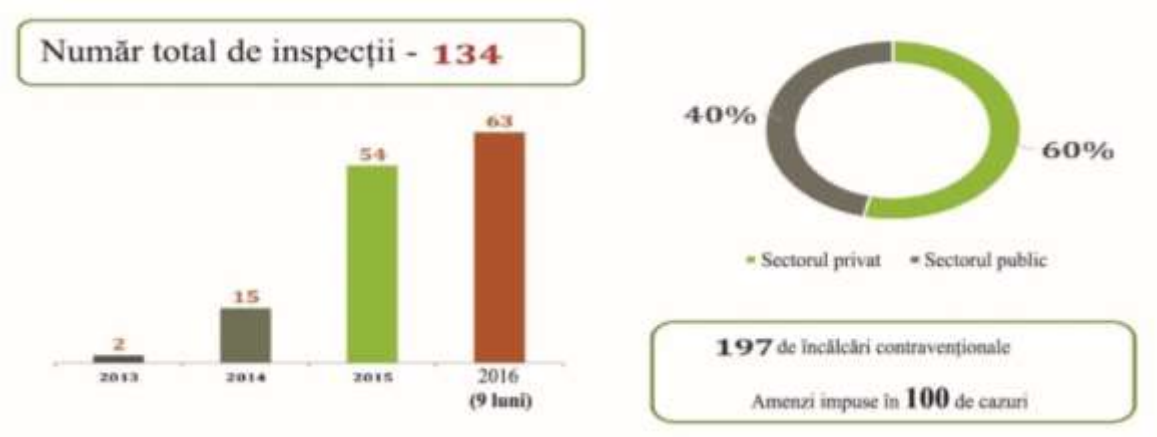
În timpul inspecției, inspectorul are dreptul de a solicita documentele de la orice persoană fizică și juridică, inclusiv informații care implică secrete comerciale și profesionale, precum și materiale care reflectă activitățile investigative operative și investigarea criminalității care sunt clasificate drept secret de stat și care sunt necesare pentru a efectua inspecția.

Operatorii de date și persoanele autorizate de aceștia sunt obligați să furnizeze inspectorului informațiile și documentele necesare imediat sau în termen de 10 zile.

Inspectorul are dreptul să verifice orice organizație și să se familiarizeze cu orice informație și documentație, indiferent de conținutul său și modul de stocare[73].

În 2016, prelucrarea datelor în următoarele instituții a fost verificată ca urmare a plângerilor depuse și inspecțiilor realizate[74][75]:

[73] https://personaldata.ge/en/about-us/what-we-do
[74] https://rm.coe.int/16806eead9
[75] https://personaldata.ge/manage/res/images/2017/angarishi/2016%20Eng.pdf



4. Ucraina

În **Ucraina**, în scopul monitorizării respectării legislației privind protecția datelor cu caracter personal, angajații Departamentului pentru Protecția Datelor cu Caracter Personal din cadrul Secretariatului Ombudsmanului efectuează inspecții programate și neprogramate ale operatorilor de date cu caracter personal (stat, întreprinderi, alte instituții și organizații, indiferent de forma juridică). Numărul inspecțiilor crește în fiecare an. În 2015 au fost efectuate 62 de inspecții, în timp ce în 2014 au existat 53 de inspecții.

În 2016 au fost realizate 76 de inspecții.
Inspecțiile fac obiectul unei proceduri speciale. Această procedură este atașată în Anexa la acest Manual.

5. Franța

În **Franța**, inspecțiile ex-post permit CNIL să verifice implementarea concretă a legii. Există stabilit un program de intervenții[76] care are în vedere evenimentele de actualitate și problemele la nivel înalt (noi tehnologii, evenimente și dezvăluiri problematice curente) asupra cărora CNIL trebuie să acționeze.

În ceea ce privește inspecțiile sau reclamațiile, CNIL a instituit un comitet restrâns (compus din 5 membri și un președinte altul decât președintele CNIL), pentru a separa puterea de reglementare de puterea de sancționare, care poate aplica diferite tipuri de sancțiuni (avertismente, sancțiuni monetare, retragerea autorizației, ordin judecătoresc etc.)[77].

Mai multe informații sunt disponibile la: https://www.cnil.fr/fr/comment-se-passe-un-controle-de-la-cnil
https://www.cnil.fr/fr/controles-en-ligne-mode-demploi

De asemenea, autoritatea irlandeză pentru protecția datelor a publicat, de exemplu, un Ghid al procesului de audit care oferă detalii privind procedurile de inspecție[78].

[76] https://www.cnil.fr/fr/programme-des-controles-2016-quelles-thematiques-prioritaires
[77] https://www.cnil.fr/en/cnils-missions
[78] https://www.dataprotection.ie/docimages/documents/GuidetoAuditProcessAug2014.pdf

3. Sancțiunile și rolul autorităților judiciare

1. Convenția 108

Protocolul adițional la **Convenția 108** prevede că autoritățile de supraveghere au competențe de investigare și intervenție, precum și competența de a se angaja în proceduri judiciare sau de a aduce la cunoștința autorităților judiciare competente încălcări ale dispozițiilor interne, aplicând principiile Convenției 108.

În conformitate cu articolul 12a al Convenției modernizate 108 propuse, autoritățile de supraveghere au competența de a lua decizii cu privire la încălcările dispozițiilor Convenției și au puterea de a impune sancțiuni administrative.

Acestea au, în același timp, puterea de a se angaja în proceduri judiciare sau de a aduce la cunoștința autorităților judiciare competente încălcări ale dispozițiilor Convenției.

2. Uniunea Europeană

În **Uniunea Europeană**, RGPD acordă competențe ample autorităților de protecție a datelor.

Acestea au competența de a aduce în fața autorităților judiciare cazurile de încălcare a prezentului regulament și, după caz, de a iniția sau de a se implica într-un alt mod în proceduri judiciare.

Mai important, acestea au puterea de a impune o amendă administrativă de până la 20 000 000 EUR sau, în cazul unei întreprinderi, până la 4 % din cifra de afaceri anuală globală totală din exercițiul financiar precedent, oricare dintre acestea este mai mare.

În conformitate cu articolul 83 din RGPD, se iau în considerare diverși factori atunci când se impune o amendă, cum ar fi de exemplu:

- natura, gravitatea și durata încălcării, ținându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum și de numărul persoanelor vizate afectate și de nivelul prejudiciilor suferite de acestea;
- dacă încălcarea a fost comisă intenționat sau din neglijență;
- orice acțiuni întreprinse de operator sau de persoana împuternicită de operator pentru a reduce prejudiciul suferit de persoana vizată;
- gradul de responsabilitate al operatorului sau al persoanei împuternicite de operator ținându-se seama de măsurile tehnice și organizatorice implementate de aceștia în temeiul articolelor 25 și 32;
- eventualele încălcări anterioare relevante comise de operator sau de persoana împuternicită de operator;
- gradul de cooperare cu autoritatea de supraveghere pentru a remedia încălcarea și a atenua posibilele efecte negative ale încălcării;
- categoriile de date cu caracter personal afectate de încălcare;

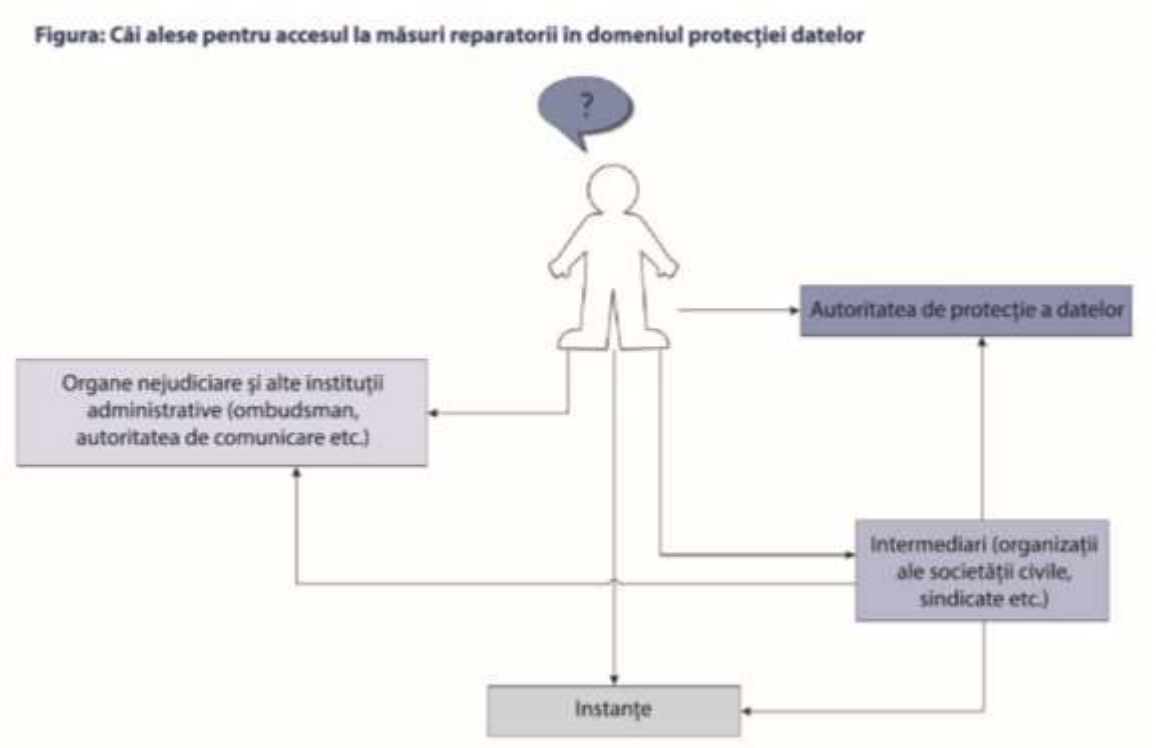
- modul în care încălcarea a fost adusă la cunoștința autorității de supraveghere, în special dacă și în ce măsură operatorul sau persoana împuternicită de operator a notificat încălcarea;
- aderarea la coduri de conduită aprobate sau la mecanisme de certificare aprobate; etc.

Sancțiunile și necesitatea de a transfera cazurile autorităților judiciare reprezintă adesea ultimul recurs utilizat de autoritățile de protecție a datelor pentru a asigura conformitatea. În multe cazuri, nu este necesară impunerea unei sancțiuni deoarece operatorul va respecta imediat recomandările sau avertismentele emise de autoritatea de supraveghere.

În orice caz, persoanele fizice au dreptul la o cale de atac și la despăgubiri pentru încălcarea dreptului la protecția datelor personale.

Agenția pentru Drepturi Fundamentale a UE a lansat în 2014 o publicație privind accesul la măsurile de protecție a datelor din statele membre ale UE[79]. Raportul conține, de exemplu, următoarea reprezentare schematică ce evidențiază rolul fundamental al autorităților de protecție a datelor:

Figura: Căi alese pentru accesul la măsuri reparatorii în domeniul protecției datelor



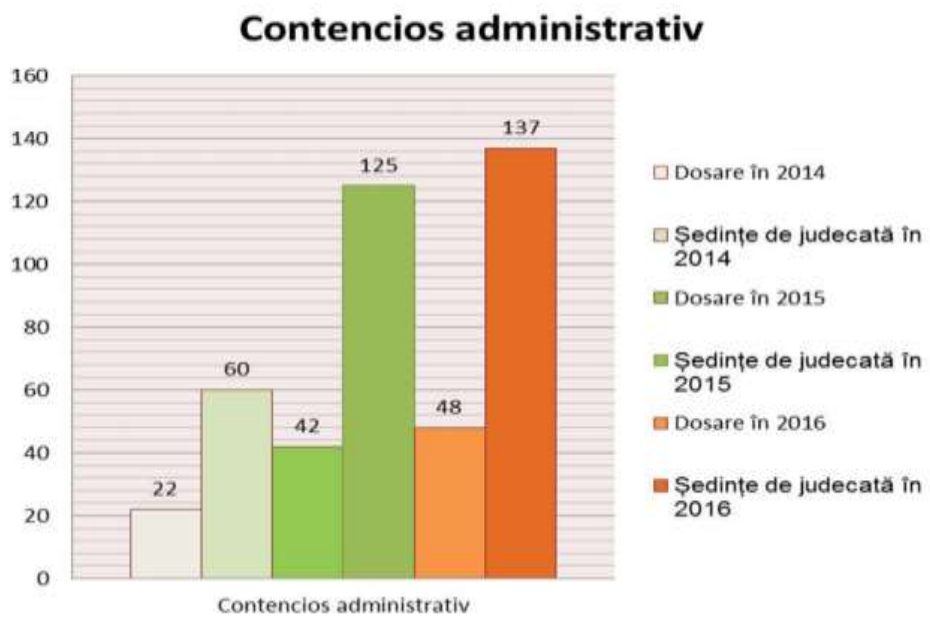
[79] http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states

3. Republica Moldova

În **Moldova**, în anul 2016, interesele Centrului au fost reprezentate în 48 de cazuri în fața instanțelor de contencios administrativ, din care: - în 5 ca intervenție auxiliară; - în 2 în calitate de petiționar; - în 41 de ani în calitate de pârât. În același timp, a fost finalizată examinarea a 10 cauze. Pentru a asigura reprezentarea autorității naționale de supraveghere în instanțele de contencios administrativ, angajații Departamentului Juridic și de Relații Publice din cadrul Centrului au participat la 137 de audieri în instanță în anul 2016[80].

În plus, în 2016, au fost înregistrate 66 contravenții și au fost încheiate 33 de procese verbale de contravenție, toate fiind trimise instanțelor competente. Prin urmare, observăm o creștere a numărului de procese verbale de contravenție comparativ cu 2015, când au fost încheiate 24 de procese verbale.

Dinamica comparativă a numărului de dosare și ședințelor de judecată în ordine de contencios administrativ, în perioada 2014-2016



4. Georgia

În **Georgia**, dacă un operator de date/ persoana împuternicită de acesta încalcă cerințele Legii, inspectorul este autorizat să dispună măsuri de executare. În particular, inspectorul are dreptul:

- de a cere eliminarea încălcărilor și a discrepanțelor aferente în termenul solicitat și în modul recomandat;
- de a cere încetarea temporară sau permanentă a prelucrării datelor;
- de a cere obstrucționarea, ștergerea, distrugerea și/ sau depersonalizarea datelor;
- de a cere încetarea fluxului transfrontalier de date;

[80] http://www.datepersonale.md/file/Raport/Raport%202016DateENG.pdf

- de a emite recomandări și instrucțiuni operatorului de date și persoanei împuternicite de acesta în cazul unor încălcări minore;
- de a se adresa instanțelor în cazul în care operatorul de date sau persoana împuternicită de acesta nu îndeplinește cererea inspectorului;
- de a impune responsabilitatea administrativă a operatorului de date și persoanei împuternicite de acesta dacă se constată contravenția;

În 2016, au fost constatate 221 de încălcări; 63 de organizații au fost sancționate cu amendă, în timp ce 35 de organizații au primit avertisment.

În domeniul marketingului direct, 48 de persoane vizate au solicitat inspectorului verificarea încălcărilor regulilor de marketing direct. În 30 de cazuri s-au constatat încălcări ale regulilor de marketing direct stabilite în lege. În 27 de cazuri, inspectorul a aplicat o amendă, iar în 3 cazuri nu s-a aplicat nicio sancțiune datorită împlinirii termenului de prescripție stabilit de lege.

Un număr mare de încălcări au vizat lipsa unui mecanism care ar permite unei persoane să renunțe la ofertele făcute prin apeluri telefonice sau SMS-uri. Lipsa de informare a persoanelor a fost, de asemenea, un domeniu major de neconformitate[81].

[81] https://personaldata.ge/manage/res/images/2017/angarishi/2016%20Eng.pdf

PARTEA 4: ACTIVITĂȚI DE EDUCARE ȘI SENSIBILIZARE

1. Uniunea Europeană

Autoritățile de protecție a datelor au obligația generală de a informa persoanele cu privire la drepturile lor, precum și operatorii și persoanele împuternicite de aceștia cu privire la obligațiile care le revin.

Agenția pentru Drepturi Fundamentale a UE reamintește că, în februarie 2008, au fost publicate două sondaje Flash Eurobarometer: „Protecția datelor în Uniunea Europeană: percepția cetățenilor”[82]; „Protecția datelor în Uniunea Europeană: percepția operatorilor”[83].

Majoritatea respondenților din UE au declarat că sunt foarte îngrijorați sau destul de îngrijorați de modul în care sunt tratate datele lor cu caracter personal.

Cea mai importantă concluzie a acestor studii a fost că majoritatea persoanelor participante au manifestat îngrijorare cu privire la aspectele legate de protecția datelor și că autoritățile naționale pentru protecția datelor erau relativ necunoscute majorității acestora.

În timp ce majoritatea respondenților păreau conștienți de drepturile lor privind utilizarea datelor cu caracter personal și de existența legislației relevante, în medie, doar 28 % dintre respondenții din UE erau conștienți de existența unei autorități naționale de protecție a datelor.

Cel mai întâlnit motiv pentru contactarea autorității naționale de protecție a datelor a fost solicitarea de îndrumare (60 % dintre respondenții care au avut contact regulat cu autoritatea pentru protecția datelor au dat acest motiv) sau formularea unei sesizări (56 %)[84].

2. Convenția 108

Convenția modernizată 108 propusă prevede în mod clar că autoritățile de protecție a datelor promovează:

- conștientizarea publică a funcțiilor și puterilor lor, precum și a activităților acestora;
- conștientizarea publică a drepturilor persoanelor vizate și exercitarea acestor drepturi;
- conștientizarea operatorilor și a persoanelor împuternicite de aceștia asupra responsabilităților lor în baza Convenției;

Se acordă o atenție deosebită drepturilor de protecție a datelor ale copiilor și ale altor persoane vulnerabile.

Autoritățile tind să dezvolte campanii de sensibilizare care vizează publicul larg prin intermediul presei, al site-ului web al autorității, al rețelelor sociale și al atelierelor specifice.

Autoritățile participă și la conferințe, seminare și ateliere pentru a informa și a fi informate, inclusiv în ceea ce privește evoluțiile TIC.

[82] http://ec.europa.eu/public_opinion/fl ash/fl_225_en.pdf
[83] http://ec.europa.eu/public_opinion/fl ash/fl_226_en.pdf
[84] http://fra.europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities

În acest sens, utilizarea site-urilor web și a rețelelor sociale devine din ce în ce mai importantă.

Raportul anual și prezentarea acestuia către presă sau către autoritățile competente reprezintă un instrument major care este valorificat de autoritățile de protecție a datelor.

3. Georgia

În **Georgia**, Oficiul pentru protecția datelor cu caracter personal oferă în mod regulat cursuri privind problemele de protecție a datelor cu caracter personal pentru reprezentanții organismelor publice și private. Se oferă cursuri nu numai pentru operatorii de date, ci și pentru orice persoană interesată de protecția datelor. Orice persoană se poate înscrie la curs prin intermediul paginii web, cursurile sunt organizate lunar și sunt gratuite.

Memorandumuri de înțelegere au fost semnate cu mai multe centre de formare ale agențiilor publice, iar problemele de protecție a datelor cu caracter personal sunt incluse în programa diferitelor programe de formare.

Oficiul pentru protecția datelor cu caracter personal oferă cursuri periodice și întâlniri de informare cu privire la aspectele legate de protecția datelor cu caracter personal, pentru a crește gradul de conștientizare a operatorilor de date și pentru a stabili o practică uniformă.

În cadrul cursurilor sunt discutate cerințele legislației privind protecția datelor, exemplele practice și cele mai bune practici din alte țări. Forma interactivă a întâlnirilor oferă oportunitatea de a ridica și a discuta problemele cele mai provocatoare și mai acute pentru public.

Oficiul cooperează fructuos cu diferite centre de formare și instituții de învățământ, cum ar fi Centrul de Formare al Justiției, Academia de Poliție și alte organizații publice și private.

Oficiul a elaborat un manual de formare de bază privind protecția datelor, precum și materiale tematice și sectoriale specifice instituțiilor publice și private.

Oficiul a organizat, de asemenea, școli de iarnă pentru studenții facultății de drept de la diferite universități din Georgia. Oficiul ține în mod regulat prelegeri publice. Au fost organizate, de asemenea, weekend-uri centrate pe tema protecției datelor pentru lectori ai facultăților de drept și jurnaliști.

4. Republica Moldova

În **Moldova**, în conformitate cu obiectivele stabilite de Strategia națională a domeniului protecției datelor cu caracter personal pentru anii 2013-2018, Centrul sporește gradul de conștientizare a opiniei publice cu privire la importanța protecției persoanelor în raport cu prelucrarea datelor cu caracter personal și informează toți operatorii asupra responsabilitățile lor.

Centrul a creat și implementat alte mijloace pentru a contribui la promovarea unei culturi a protecției datelor cu caracter personal, cum ar fi conferințe, dezbateri, ateliere, spoturi video, comunicarea cu utilizatorii prin ziare, radio, televiziune, rețele sociale, site-uri web etc[85].

5. Ucraina

În **Ucraina**, de exemplu, Departamentul Comisarului a organizat „Școala de protecție a datelor cu caracter personal" și alte seminare în cadrul cărora participanții au avut ocazia să dobândească cunoștințe despre legislația Ucrainei privind protecția datelor.

„Școala de protecție a datelor cu caracter personal" este un curs de trei zile, în cadrul căruia participanții participă la prelegeri ținute de angajații Departamentului pentru Protecția Datelor cu Caracter Personal din cadrul Secretariatului Ombudsmanului. În cadrul colocviilor, participanții pot testa cunoștințele pe care le-au dobândit.

Mai mult, manualul „Protecția datelor cu caracter personal: reglementare juridică și aspecte practice" a fost publicat în cadrul proiectului comun al Uniunii Europene și al Consiliului Europei „Consolidarea societății informaționale în Ucraina".

În plus, au fost tipărite diferite broșuri în domeniul protecției datelor cu caracter personal, inclusiv „*Ce ar trebui să cunoască subiecții datelor cu caracter personal*" și „Ce ar trebui să cunoască operatorii și persoanele împuternicite de aceștia".

6. Grupul de Lucru Educație Digitală

Se poate menționa, mai specific, activitatea **Grupului de Lucru Educație Digitală (DEWG) din cadrul Conferinței Internaționale a Comisarilor pentru Protecția Datelor și a Vieții Private**, organizată de-a lungul mai multor ani. DEWG a creat instrumentele necesare pentru ca autoritățile să intervină în educația digitală disponibilă omologilor și a ajutat la implantarea unei culturi de partajare a experienței în acel spațiu[86].

[85] http://www.datepersonale.md/file/Raport/Raport%202016DateENG.pdf
[86] https://icdppc.org/document-archive/working-group-reports/

PARTEA 5: ACTIVITĂȚI DE COOPERARE INTERNAȚIONALĂ

Din ce în ce mai mult, provocările cu care se confruntă autoritățile de protecție a datelor conțin o dimensiune internațională.

Cooperarea internațională a devenit o necesitate absolută pentru autoritățile de supraveghere, fie prin cooperarea bilaterală a autorităților, fie prin cooperarea multilaterală.

1. Cooperare

Cooperarea internațională poate fi în primul rând încurajată prin **cooperarea bilaterală** directă între două autorități.

De exemplu, la 10 octombrie 2016 a fost semnat un acord de cooperare între Inspectoratul pentru protecția datelor cu caracter personal din Georgia și Centrul Național pentru Protecția Datelor din Republica Moldova.

De asemenea, pot fi organizate vizite de studiu și schimburi de membri ai personalului între autoritățile de protecție a datelor pentru a facilita cooperarea și schimbul de informații relevante.

2. Convenția 108

Protocolul adițional la Convenția 108 prevede clar că „autoritățile de supraveghere cooperează între ele în măsura necesară pentru îndeplinirea sarcinilor lor, în special prin schimbul de informații utile".

Convenția 108 stabilește un **Comitet consultativ** format din reprezentanți ai Părților la Convenție, completat de observatori din alte state și organizații internaționale, actori nestatali, care este responsabil de interpretarea dispozițiilor și de îmbunătățirea punerii în aplicare a Convenției.

De asemenea, acest Comitet este responsabil de elaborarea rapoartelor, orientărilor și principiilor directoare pe o largă varietate de subiecte[87].

Propunerea pentru **o Convenție 108 modernizată** încurajează, de asemenea, cooperarea dintre autoritățile de supraveghere, în special prin:
a. furnizarea de asistență reciprocă prin schimbul de informații relevante și utile și cooperarea reciprocă;
b. coordonarea investigațiilor sau intervențiilor sau desfășurarea de acțiuni comune;
c. furnizarea de informații și documente privind legislația și practica administrativă referitoare la protecția datelor.

[87] http://www.coe.int/en/web/data-protection/-consultative-committee-t-pd

3. Uniunea Europeană

La nivelul **Uniunii Europene**, **Grupul de lucru în temeiul articolului 29** este un grup de lucru european independent care se ocupă de aspecte legate de protecția vieții private și a datelor cu caracter personal. Autoritățile de protecție a datelor din cele 28 de state membre ale UE sunt membre ale Grupului de lucru. În afară de statele membre UE, și Autoritatea Europeană pentru Protecția Datelor participă în activitățile Grupului de lucru. Statele membre ale Spațiului Economic European (Islanda, Liechtenstein și Norvegia) au statut de observator în acest grup, la fel ca numeroase alte state membre candidate.

Misiunile Grupului de Lucru în temeiul articolului 29 cuprind toate aspectele legate de aplicarea dispozițiilor naționale adoptate în aplicarea Directivei 95/46/CE (Directiva privind protecția datelor) și a Directivei 2002/58/ CE (Directiva privind comunicațiile electronice).

Grupul de lucru în temeiul articolului 29 emite în mod regulat avize, publică documente de lucru și rezoluții privind diferite subiecte legate de protecția vieții private și a datelor cu caracter personal. Aproape 250 de documente au fost adoptate de Grupul de lucru[88].

Grupul de lucru în temeiul articolului 29 întocmește un plan de lucru pe doi ani, iar raportul său anual de activitate este, de asemenea, public și disponibil online.

Grupul de lucru în temeiul articolului 29 organizează o sesiune plenară de două zile la Bruxelles, de cinci ori pe an.

Odată cu viitorul **RGPD**, se aplică reguli solide de cooperare între autorități și de asistență reciprocă. Sunt permise operațiuni comune ale autorităților de supraveghere. În plus, se prevede un mecanism de coerență, iar Grupul de lucru în temeiul articolului 29 va fi înlocuit de **Comitetul european pentru protecția datelor**, care va avea, în anumite cazuri transfrontaliere, competența de a emite avize obligatorii[89].

4. Conferința Internațională a Comisarilor pentru Protecția Datelor și a Vieții Private

În fiecare an, **Conferința Internațională a Comisarilor pentru Protecția Datelor și Confidențialitate** are loc într-un alt oraș găzduit de o autoritate de protecție a datelor sau responsabilă de confidențialitate. Conferința a avut loc pentru prima dată în Bonn, Germania, în 1979 și apoi a trecut Atlanticul, pentru cea de-a doua întâlnire, în Ottawa, Canada.

Conferința este o entitate care reprezintă membrii colectivi acreditați, care sunt autorități publice ce îndeplinesc criteriile de aderare stabilite în regulile și procedurile conferințelor. În prezent există 119 autorități de protecție a datelor și responsabile de confidențialitate acreditate ca membri ai conferinței.

Conferința urmărește:

[88] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
[89] http://eur-lex.europa.eu/legal-content/ro/TXT/HTML/?uri=CELEX:32016R0679&from=ro

- să fie un forum mondial remarcabil pentru autoritățile de protecție a vieții private și a datelor;
- să difuzeze cunoștințe și să ofere asistență practică pentru a ajuta autoritățile să-și îndeplinească mai eficient mandatele;
- să asigure funcția de conducere la nivel internațional în domeniul protecției și confidențialității datelor;
- să conecteze și să sprijine eforturile la nivel național și regional și în alte forumuri internaționale, pentru a permite autorităților să protejeze mai bine și să promoveze confidențialitatea și protecția datelor.

Standardele internaționale privind protecția datelor cu caracter personal și confidențialitatea au fost adoptate în 2009 în cadrul conferinței organizate la Madrid[90].

Acordul de cooperare transfrontalieră privind aplicarea transfrontalieră globală a fost adoptat la Mauritius cu ocazia celei de-a 36-a conferințe (2014).

5. Grupul de lucru internațional privind protecția datelor în domeniul telecomunicațiilor

Grupul de lucru internațional privind protecția datelor în domeniul telecomunicațiilor („Grupul de la Berlin") a fost înființat în 1983 în cadrul Conferinței internaționale a comisarilor pentru protecția datelor și a vieții private.

Grupul de lucru reunește experți în domeniul telecomunicațiilor - experți juridici și tehnici - ai autorităților de protecție a datelor și alți actori din sectorul telecomunicațiilor. Reuniunile sunt organizate de două ori pe an, una în Berlin și una la invitația unui membru al grupului. De la înființare, Grupul de la Berlin a adoptat numeroase documente și rezoluții menite să sporească nivelul de atenție privind protecția datelor în sectoarele de telecomunicații și internet[91].

6. Conferința Europeană pentru Protecția Datelor

Autoritățile de protecție a datelor din statele membre ale UE și din unele state membre ale Consiliului Europei se reunesc anual la **Conferința europeană pentru protecția datelor** („Conferința de primăvară").

Participanții la conferință dezbat numeroase subiecte legate de protecția datelor în cadrul reuniunilor plenare, fac schimb de metode de lucru și pot adopta rezoluții pe diverse teme.

Două grupuri de lucru stabilite la conferință sunt dedicate unor teme mai specifice:

- „„Grupul de lucru pentru poliție și justiție";;
- „Atelierele de gestionare a cazurilor": ateliere internaționale pentru angajații autorităților de protecție a datelor, care se desfășoară de două ori pe an și care vizează schimbul de informații și de experiență în cazuri concrete.

[90] https://icdppc.org/

[91] https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

7. Autoritățile de protecție a datelor cu caracter personal din Europa Centrală și de Est

La sfârșitul anului 2001, în cadrul unei conferințe internaționale organizate de Consiliul Europei, a fost inițiată o cooperare internațională între **autoritățile de protecție a datelor cu caracter personal din Europa Centrală și de Est (CEEDPA).**

Întâlnirile autorităților de protecție a datelor cu caracter personal din Europa Centrală și de Est, menite să sprijine schimbul de informații și experiență, sensibilizarea cu privire la protecția datelor cu caracter personal, precum și armonizarea în continuare a dispozițiilor naționale cu legea au avut loc sub forma unor conferințe periodice organizate în anumite țări[92].

Cea de-a 19-a reuniune a autorităților de protecție a datelor din Europa Centrală și de Est a avut loc în perioada 17-18 mai 2017 la Tbilisi, în Georgia.

8. Grupul de lucru pentru securitate și confidențialitate în economia digitală

La nivelul **Organizației pentru Cooperare și Dezvoltare Economică (OCDE), Grupul de lucru pentru securitate și confidențialitate în economia digitală (SPDE)**[93], fostul Grup de lucru pentru securitatea și confidențialitatea informațiilor (WPISP) elaborează o analiză a politicilor publice și recomandări pentru a ajuta guvernele și alte părți interesate să se asigure că securitatea digitală și protecția vieții private promovează dezvoltarea economiei digitale.

Merită notat că au fost adoptate recomandări, de exemplu, în următoarele domenii[94]:
- 2016: Recomandarea Consiliului privind guvernanța datelor privind sănătatea;
- 2015: Recomandarea Consiliului privind managementul riscurilor de securitate digitală;
- 2013: Recomandarea Consiliului privind orientările pentru protecția vieții private și a fluxurilor transfrontaliere de date cu caracter personal;
- 2012: Recomandarea Consiliului privind protecția copiilor în mediul on-line;
- 2011: Recomandarea Consiliului privind principiile de elaborare a politicilor pe internet.

În iunie 2007, guvernele parte la OCDE au adoptat și o **Recomandare pentru cooperare transfrontalieră în aplicarea legilor de protecție a vieții private**. Recomandarea a solicitat țărilor membre să promoveze crearea unei rețele informale de autorități de aplicare a legislației în materie de confidențialitate.

Rețeaua globală de asigurare a respectării vieții private (GPEN - Global Privacy Enforcement Network) a fost creată pentru a consolida protecția vieții private într-un context global. GPEN conectează autoritățile din domeniul protecției vieții private din întreaga lume pentru a promova și sprijini cooperarea în aplicarea transfrontalieră a legilor care protejează viața privată.

Se urmărește, în primul rând, promovarea cooperării prin:
- schimbul de informații despre aspecte, tendințe și experiențe relevante;

[92] www.ceecprivacy.org
[93] http://www.oecd.org/sti/ieconomy/workingpartyonsecurityandprivacyinthedigitaleconomyspde.htm
[94] http://www.oecd.org/sti/ieconomy/security-and-privacy-resources.htm

- încurajarea oportunităților de formare și împărtășire a know-how-ului, expertizei și bunelor practici;
- promovarea dialogului cu organizațiile care au un rol în domeniul respectării vieții private;
- crearea, menținerea și susținerea unor procese sau mecanisme utile pentru cooperarea bilaterală sau multilaterală[95].

9. Organizația Internațională de Standardizare

Organizația Internațională de Standardizare (ISO - International Organisation for Standardisation) este o organizație internațională independentă și neguvernamentală care are ca membri un număr de 163 de organisme naționale de standardizare[96].

Aceasta reunește experți pentru a împărtăși cunoștințe și a dezvolta standarde internaționale voluntare și consensuale. Aceste standarde intenționează să ofere specificații pentru produse, servicii și sisteme, pentru a asigura calitatea și siguranța, facilitând în același timp comerțul internațional.

Standarde ISO au fost elaborate și în domeniul vieții private. Se pot menționa, de exemplu, următoarele standarde:

- ISO/ CEI 29100 Tehnologia informației - Tehnici de securitate - Cod de practică pentru managementul securității informațiilor;
- ISO/ CEI 29101 Tehnologia informației - Tehnici de securitate - Cadrul arhitecturii de securitate a informațiilor;
- ISO/ CEI 27001 Tehnologia informației - Tehnici de securitate - Sisteme de management pentru securitatea informației - Cerințe;
- ISO/ CEI 27002 Tehnologia informației - Tehnici de securitate - Cod de practică pentru managementul securității informatice;
- ISO/ IEC 27018 Tehnologia informației - Tehnici de securitate - Cod de practică pentru protejarea informațiilor de identificare personală (PII) în cloud public care acționează ca prelucrător PII;
- ISO/ IEC 29134 Tehnologia informației - Tehnici de securitate - Orientări pentru evaluarea impactului asupra vieții private; etc.

10. Asociația francofonă a autorităților de protecție a datelor

Asociația francofonă a autorităților de protecție a datelor („Association francophone des autorités de protection des données personnelles" sau AFAPDP) a fost înființată în anul 2007 și reunește autorități de protecție a datelor din 18 țări membre în „Organisation Internationale de la Francophonie" (OIF)[97].

Această organizație are sarcina de a promova inițiativele de cooperare și formare între țările vorbitoare de limbă franceză în domeniul protecției datelor. Aceasta dorește să ofere spațiu

[95] https://www.privacyenforcement.net/public/activities
[96] https://www.iso.org/fr/home.html
[97] http://www.afapdp.org/

pentru îndrumare și schimburi către noile autorități de protecție a datelor și este o sursă de expertiză pentru țările care nu au încă o legislație privind protecția datelor.

În fiecare an, AFAPDP organizează o întâlnire pentru toți membrii săi și organizează un seminar colectiv anual destinat ca for pentru schimbul de informații și discutarea temelor actuale.

11. Rețeaua ibero-americană pentru protecția datelor

Rețeaua ibero-americană pentru protecția datelor (RIPD) a rezultat în urma acordului încheiat la Simpozionul ibero-american privind protecția datelor (EIPD), care a avut loc în Guatemala în iunie 2003, cu participarea a 12 țări ibero-americane.

RIPD a fost creat ca un for pentru promovarea dreptului la protecția datelor în comunitatea ibero-americană.

RIPD vizează promovarea dezvoltării legale și instituționale a protecției datelor în țările ibero-americane.

Rețeaua lucrează, de asemenea, la cooperarea prin schimbul de informații, experiență și cunoștințe în dezvoltarea instrumentelor comune și implicând activități coordonate/ comune[98].

12. Cooperarea economică Asia-Pacific

Cooperarea economică Asia-Pacific (APEC) este un for economic regional, înființat în 1989, pentru a stimula interdependența din Asia-Pacific. APEC reunește 21 de membri.

Aceasta vizează facilitarea comerțului transfrontalier, precum și dezvoltarea comerțului electronic în zonă.

„Cadrul de confidențialitate APEC”, adoptat în 2004, promovează o abordare flexibilă a protecției vieții private din toate statele membre ale APEC. Cadrul stabilește un set comun de principii privind confidențialitatea și oferă asistență tehnică acelor economii care încă nu abordează confidențialitatea din punct de vedere al reglementării sau al politicii[99].

[98] http://www.redipd.org/index-ides-idphp.php
[99] http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

Anexa 1: Formularul elaborat de Comisarul Parlamentului Ucrainean pentru Drepturile Omului pentru prelucrarea datelor cu caracter personal cu riscuri speciale pentru drepturile și libertățile persoanelor vizate

Aprobat prin
Decretul Comisarului
Parlamentului Ucrainei
pentru Drepturile Omului
_____ ianuarie 2014 nr. _____

Cerere de prelucrare a datelor cu caracter personal, cu riscuri speciale pentru drepturile și libertățile persoanelor vizate *

***Cererea se completează cu litere de tipar**

1 Numele complet/ Denumirea operatorului de date cu caracter personal

---

USREOU/ Numărul de înregistrare al cardului de înregistrare al contribuabilului												

Numărul și seria pașaportului												

Autoritatea emitentă și data emiterii

Locația (pentru persoane juridice)/ Locul de reședință (pentru persoane fizice)	

---

2. Prelucrarea datelor date cu caracter personal:

□ origine rasială	□ origine etnică	□ origine națională	
□ convingeri politice	□ convingeri religioase	□ convingeri ideologice	
□ apartenența la partide și/sau organizații politice	□ apartenența la sindicate	□ apartenența la organizații religioase	□ apartenența la organizații publice de orientare ideologică

□ starea de sănătate	□ viața sexuală	□ date biometrice	□ date genetice
□ răspunderea contravențională	□ răspunderea penală	□ aplicarea de măsuri în cursul anchetei preliminare	□ măsurile luate în baza Legii Ucrainei „privind activitățile de cercetare operativă”
□ comiterea anumitor tipuri de violențe împotriva persoanelor	□ locația și/sau mișcarea persoanelor		

3. Categoria sau categoriile de persoane vizate ale căror date cu caracter personal sunt prelucrate:

---

4. Scopul prelucrării datelor date cu caracter personal cu trimitere la acte normative, reglementări, acte constitutive sau alte documente care reglementează activitatea operatorului de date cu caracter personal:

---

5. Numele/denumirea completă a operatorului de date cu caracter personal *

USREOU/ Numărul de înregistrare al cardului de înregistrare al contribuabilului												
Numărul și seria pașaportului												

Datele pașaportului și data emiterii

Locația (pentru persoane juridice)/ Locul de reședință (pentru persoane fizice)	

*** Se completează pentru fiecare administrator de date cu caracter personal**

6. Informații privind terții către care sunt transferate date cu caracter personal*

☐ Datele cu caracter personal sunt transferate către terți	☐ Datele cu caracter personal nu sunt transferate către terți

7. Informații privind transferul transfrontalier al datelor cu caracter personal

☐ nu s-a realizat	☐ s-a realizat

7.1 Țara (țările) în care sunt transferate date cu caracter personal:

7.2 Informații privind relația cu entitatea străină/ entitățile străine către care sunt transferate date cu caracter personal:

7.3 Scopul transferului transfrontalier de date cu caracter personal

7.4 Temeiul juridic al transferului transfrontalier de date cu caracter personal:

8. Descriere generală a măsurilor tehnice și organizatorice întreprinse de operatorul de date cu caracter personal în scopul protejării acestora:

9. Locația (adresa reală) a prelucrării datelor cu caracter personal:

Loc pentru ștampilă _____

semnătură, /denumire completă, funcție/

Pagina ☐ Total pagini ☐

Anexa 2: Procedură pentru inspecțiile desfășurate de Comisarul Parlamentului Ucrainei pentru Drepturile Omului

Aprobat prin
Decretul Comisarului
Parlamentului Ucrainei
pentru Drepturile Omului
8 ianuarie 2014 nr. 1/02-14

Procedură
pentru controlul exercitat de Comisarul Parlamentului Ucrainei pentru Drepturile Omului asupra respectării legislației privind protecția datelor cu caracter personal

1. Dispoziții generale

1.1. Procedura de față prevede mecanismul de control al Comisarului Parlamentului Ucrainei pentru Drepturile Omului (denumit în continuare - Comisarul) relativ la respectarea cerințelor legale privind protecția datelor cu caracter personal prin efectuarea de inspecții la persoane fizice, antreprenori persoane fizice, întreprinderi, instituții și organizații sub orice formă juridică, autorități centrale și locale care dețin și/ sau administrează date cu caracter personal (denumită în continuare - subiectul inspecției), precum și redactarea și revizuirea rezultatelor inspecțiilor.
1.2. În această Procedură, următorii termeni au următoarele definiții:
Inspecție la distanță - inspecția programată sau neprogramată a activității persoanei care face obiectul inspecției de către comisar și/sau de către funcționarii desemnați, efectuată la sediul Secretariatului Comisarului Parlamentului Ucrainei pentru Drepturile Omului, pe baza documentelor primite de la persoana care face obiectul inspecțiilor și pe baza explicațiilor, fără a se deplasa la locul unde se află respectiva persoană care face obiectul inspecției și/sau la locul unde sunt prelucrate datele cu caracter personal;
Inspecția în teren - verificarea programată sau neprogramată a activității persoanei care face obiectul inspecției de către comisar și/sau de către funcționarii desemnați de acesta, efectuată la locul unde se află persoana care face obiectul inspecției și/sau direct la locul unde sunt prelucrate datele cu caracter personal;
Inspecție programată - inspecția activității persoanei care face obiectul inspecției, efectuate în conformitate cu planul de inspecții întocmit pentru un anumit trimestru și an;
Inspecție neprogramată - inspecția activității persoanei care face obiectul inspecției, care nu este prevăzută în planul de inspecție.
Actul de inspecție - document intern care atestă efectuarea inspecției activității persoanei care face obiectul inspecției și situația respectării cerințelor legislației privind protecția datelor cu caracter personal de către această persoană;
Ordin de îmbunătățire (cerință) - este obligatoriu pentru respectarea cerințelor stabilite de Comisarul pentru drepturile omului privind încetarea încălcării cerințelor stabilite de legislația privind protecția datelor cu caracter personal, prezentat (trimis) persoanei care face obiectul inspecției.
Alți termeni prevăzuți în această procedură vor fi utilizați în conformitate cu Legea Ucrainei „cu privire la protecția datelor cu caracter personal".

2. Organizarea și desfășurarea inspecțiilor

2.1. Controlul asupra respectării legislației privind protecția datelor cu caracter personal de către subiecții inspecțiilor se realizează de către comisar și/ sau funcționarii desemnați de acesta prin efectuarea de inspecții: programate, neprogramate, în teren și la distanță. Inspecțiile programate și neprogramate pot fi efectuate în teren sau la distanță.
Obiectul inspecției este respectarea cerințelor Constituției Ucrainei, a Legii Ucrainei „cu privire la protecția datelor cu caracter personal", a unei proceduri model pentru prelucrarea datelor cu caracter personal, precum și a tratatelor internaționale în vigoare ale Ucrainei în domeniul datelor cu caracter personal, pe care Parlamentul Ucrainei le-a convenit, de către persoana care face obiectul inspecției la prelucrarea datelor cu caracter personal.

2.2 Verificarea în teren este efectuată de către Comisarul pentru Drepturile Omului al Parlamentului Ucrainei și/ sau de către următorii funcționari autorizați (denumiți în continuare „funcționari autorizați”):

– șeful Secretariatului Comisarului Parlamentului Ucrainei pentru Drepturile Omului și adjunctul acestuia;
– reprezentanții Comisarului Parlamentului Ucrainei pentru Drepturile Omului;
– șefii de departamente și adjuncții acestora;
– alți angajați ai Secretariatului Comisarului Parlamentului Ucrainei pentru Drepturile Omului.

Funcționarii autorizați își exercită autoritățile în baza identificării oficiale și a suplimentului, care reprezintă o parte indispensabilă a permisului de trecere și confirmă volumul autorităților angajatului Secretariatului Comisarului Parlamentului Ucrainei pentru Drepturile Omului, în conformitate cu Regulamentul privind identificarea oficială a angajaților Secretariatului Comisarului Parlamentului Ucrainei pentru Drepturile Omului, aprobat prin Decretul Comisarului Parlamentului Ucrainei pentru Drepturile Omului din 14 decembrie 2012 nr. 19/ 8-12.

2.3. Funcționarii autorităților de stat, inclusiv organele administrației publice, organele executive și organele judiciare, pot fi implicați în inspecție în conformitate cu ordinea stabilită de legislație. În cazul în care sunt implicate persoanele specificate, acestea trebuie să prezinte o obligație scrisă privind nedivulgarea datelor cu caracter personal pe care acestea le dobândesc ca urmare a inspecției.
2.4. Inspecțiile în teren se efectuează în cursul programului de lucru al persoanei care face obiectul inspecției, stabilit de reglementările interne în domeniul muncii.
2.5. La efectuarea inspecției, Comisarul, funcționarul desemnat și persoana care face obiectul inspecției au drepturile și obligațiile prevăzute în secțiunea 6 a prezentei proceduri.
2.6. Persoana care face obiectul inspecției este obligată să asigure accesul la spațiile, materialele și documentele necesare desfășurării unei inspecții, să furnizeze informații și explicații privind situația de fapt și temeiul juridic al acțiunilor și deciziilor sale, precum și să asigure condițiile relevante pentru efectuarea unei analize asupra acestor informații.
2.7. Inspecția la distanță va fi efectuată de către Comisar și/sau funcționarii desemnați în ordinea stabilită la punctele

3. Desfășurarea unei inspecții programate

3.1-3.6 din secțiunea 3 a Procedurii de desfășurare a inspecțiilor de către Comisarul Parlamentului Ucrainei pentru drepturile omului, ținând seama de dispozițiile prezentei proceduri.
3.1. Inspecțiile programate se efectuează în conformitate cu planurile anuale sau trimestriale aprobate de Comisar înainte de data de 1 decembrie a anului care precede anul vizat sau înainte de data de 25 a ultimei luni care precede trimestrul vizat.
3.2. Planul trebuie să includă categoriile de persoane care pot fi supuse inspecțiilor. După aprobare, planul de inspecție va fi publicat pe site-ul oficial al Comisarului.
3.3. Inspecțiile programate la o persoană care face obiectul inspecției cu privire la respectarea cerințelor legislației în domeniul protecției datelor cu caracter personal se efectuează periodic, dar nu mai mult de o dată pe an.
3.4. Data care definește termenul până la începerea noii inspecții este data finală a inspecției anterioare programate.

4. Desfășurarea unei inspecții neprogramate

4.1. Inspecțiile neprogramate la persoanele care fac obiectul inspecției pot fi efectuate pe baza existenței unuia sau a mai multor temeiuri/ motive, în special:
La inițiativa Comisarului pentru drepturile omului;
În cazul în care Comisarul pentru drepturile omului a descoperit în mod direct încălcări ale cerințelor legislației privind protecția datelor cu caracter personal, inclusiv ca rezultat al cercetării problemelor sistemice privind respectarea drepturilor la confidențialitate, respectarea vieții private și de familie;
Pe baza informațiilor privind încălcările cerințelor legislației privind protecția datelor cu caracter personal în publicațiile disponibile în mass-media sau pe Internet;
În baza petițiilor bine întemeiate ale persoanelor fizice și juridice care au sesizat încălcarea cerințelor legislației privind protecția datelor cu caracter personal, act săvârșit de o persoană fizică, un antreprenor persoană fizică, întreprindere, instituție și organizație cu orice formă juridică, autorități centrale sau locale care dețin și/ sau gestionează date cu caracter personal;
Atunci când informațiile furnizate de persoana care face obiectul inspecției ca răspuns la solicitarea Comisarului pentru drepturile omului în urma unei inspecții la distanță au fost false și/sau dacă aceste informații (date) nu oferă

posibilitatea de a evalua modul în care persoana care face obiectul inspecției îndeplinește cerințele legislației privind protecția datelor cu caracter personal;
Controlul privind executarea de către persoana care face obiectul inspecției a ordinelor de îmbunătățire referitoare la eliminarea încălcărilor cerințelor legislației privind protecția datelor cu caracter personal, emise ca urmare a inspecțiilor efectuate.

5. Redactarea rezultatelor inspecțiilor

5.1. Cu privire la rezultatele inspecției programate sau neprogramate, Comisarul și/sau funcționarul desemnat întocmește/întocmesc actul de control asupra respectării cerințelor legislației privind protecția datelor cu caracter personal (denumit în continuare - Actul) în două exemplare, pe baza formularului stabilit în Suplimentul 1 la această Procedură.
5.2. Actul trebuie să includă următoarele informații:
data, ora și locul redactării;
funcțiile, numele și semnăturile persoanelor care au efectuat inspecția;
funcția, numele și semnătura conducătorului persoanei care face obiectul inspecției (funcționarul desemnat de acesta) sau numele și semnătura unei persoane fizice care face obiectul inspecției;
tipul inspecției (programată, neprogramată, în teren, la distanță);
pentru persoana care face obiectul inspecției - organ al autorității centrale sau locale: denumirea, locația;
pentru persoana care face obiectul inspecției - persoană juridică: denumire, locație;
pentru persoana care face obiectul inspecției - persoană fizică și/sau persoană fizică autorizată: numele, prenumele și patronimicul, locul înregistrării;
informații privind data, ora de începere și finalizare a inspecției, durata sa totală;
fapte (condiții) constatate pe baza rezultatelor inspecției;
concluzii privind rezultatele inspecției.
La întocmirea Actului, trebuie să fie respectată obiectivitatea și caracterul complet al descrierii constatărilor și datelor.
5.3. Actul va include una dintre următoarele concluzii:
cu privire la absența încălcărilor cerințelor legislației privind protecția datelor cu caracter personal în activitatea persoanei care face obiectul inspecției;
cu privire la încălcarea legislației privind protecția datelor cu caracter personal de către persoana care face obiectul inspecției, descrierea detaliată a acesteia cu referire la normele legislative în vigoare încălcate;
Este interzisă includerea în Act a informațiilor privind încălcările care nu sunt dovedite de documente.
5.4. Actul include tot ceea ce s-a stabilit în timpul inspecțiilor privind neexecutarea (executarea necorespunzătoare) a cerințelor legislației privind datele cu caracter personal de către persoana care face obiectul inspecției.
5.5. În cazul în care persoana care face obiectul inspecției nu furnizează documentele necesare pentru efectuarea inspecției, Actul trebuie să includă acest fapt și motivele.

5.6. Inspecția în teren
5.6.1. Pe baza rezultatelor inspecției efectuate în teren, Actul se întocmește în două exemplare și se semnează de Comisar sau de funcționarul desemnat de acesta care a efectuat inspecția, precum și de conducătorul subiectului inspecției sau de persoana desemnată de acesta.
5.6.2. Dacă persoana care face obiectul inspecției nu este de acord cu acest Act, aceasta îl semnează, consemnând observațiile sale. Observațiile persoanei care face obiectul inspecției privind procesul de control al respectării cerințelor legislației privind protecția datelor cu caracter personal de către funcționarii desemnați fac parte integrantă din Act. După aceea, ultima pagină a tuturor exemplarelor Actului va include mențiunea: „Cu observații".
În cazul în care conducătorul persoanei care face obiectul inspecției nu este de acord să semneze Actul, funcționarul desemnat include o notă relevantă în acest sens în Act.
5.6.3. Primul exemplar al Actului va fi înaintat conducătorului subiectului inspecției sau persoanei desemnate, prin semnarea celui de-al doilea exemplar al Actului, care va fi ținut la Secretariatul Comisarului.
În cazul în care conducătorul persoanei care face obiectul inspecției sau persoana desemnată de acesta refuză să primească cel de-al doilea exemplar al Actului, acesta va fi comunicat persoanei care face obiectul inspecției în termen de 5 zile lucrătoare printr-o scrisoare recomandată cu confirmare de primire.
Exemplarul Actului, păstrat la Secretariatul Comisarului, se completează cu materialele inspecției - copii ale documentelor, extrase din documentele certificate în mod corespunzător de persoana care face obiectul inspecției, explicații, procese verbale și alte documente.

5.7. Inspecția la distanță
5.7.1. Pe baza rezultatelor inspecției efectuate la distanță, Actul se întocmește în două exemplare și se semnează de către Comisar sau de către funcționarul desemnat de acesta, care a efectuat inspecția. Primul exemplar va fi comunicat spre analiză persoanei care face obiectul inspecției, iar cel de-al doilea va fi păstrat la Secretariatul Comisarului.
5.7.2. Exemplarul Actului păstrat la Secretariatul Comisarului se completează cu materialele inspecției - copii ale documentelor, extrase din documentele certificate în mod corespunzător de persoana care face obiectul inspecției, explicații, procese verbale și alte documente.

5.8. Nu se permite nicio corecție sau completare a Actului de inspecție după semnarea acestuia. Persoana care face obiectul inspecției este informată în scris cu privire la constatarea abaterilor după semnarea actului.
5.9. Orice informație pe care comisarul și/sau funcționarul desemnat de acesta o iau la cunoștință în timpul inspecției este supusă clauzei de nedivulgare.
5.10. Pe baza actului de inspecție în cursul căruia s-au constatat încălcări ale cerințelor legislației privind protecția datelor cu caracter personal, un ordin de îmbunătățire și de eliminare a încălcărilor cerințelor legislației în domeniul protecției datelor cu caracter personal care au fost constatate în timpul inspecției este eliberat conform formularului stabilit în Suplimentul 2 la prezenta Procedură (denumit în continuare Ordin).
5.11. Ordinul va cuprinde:
numărul, data și locul în care a fost emis ordinul;
pentru persoana care face obiectul inspecției - organ al autorității centrale sau locale: denumirea, locația;
Pentru persoana care face obiectul inspecției - persoană juridică: denumirea, locația, prenumele, numele și patronimicul conducătorului entității juridice;
pentru persoana care face obiectul inspecției - persoană fizică și/sau persoană fizică autorizată: numele, prenumele și patronimicul, locul de reședință;
motivele emiterii Ordinului;
măsurile necesare pentru a elimina încălcările constatate în cursul inspecției;
termenul pentru executarea Ordinului;
termenul pentru informarea Comisarului cu privire la eliminarea încălcării constatate, de către persoana care face obiectul inspecției;
semnătura funcționarului(funcționarilor) desemnat(desemnați) care a(au) efectuat inspecția.
5.12. Ordinul se eliberează în două exemplare: primul exemplar se trimite subiectului inspecției sau persoanei desemnate de acesta printr-o scrisoare recomandată cu confirmare de primire în termen de 5 zile lucrătoare de la data întocmirii Actului de inspecție, iar al doilea exemplar rămâne la Secretariatul Comisarului.
Exemplarul care rămâne la Secretariatul Comisarului va avea numărul de referință și data trimiterii corespunzătoare.
5.13. Persoana care face obiectul inspecției trebuie să ia măsuri pentru eliminarea încălcărilor definite de Ordin în termenul stabilit de Ordin (minimum 30 de zile calendaristice) și să informeze Comisarul în scris cu privire la eliminarea încălcărilor, furnizând de asemenea copii ale documentelor care dovedesc acest lucru.
5.14. Controlul asupra oportunității și caracterului complet al îndeplinirii cerințelor stipulate în Ordin este exercitat prin analiza copiilor documentelor menționate mai sus și, în caz de necesitate, printr-o inspecție neprogramată.
5.15. În caz de nerespectare a Ordinului în termenul stabilit în acesta, Comisarul sau funcționarul desemnat de acesta întocmește un proces verbal de contravenție prevăzut la articolul 188^{40} din Codul Civil al Ucrainei privind contravențiile (în continuare - CUoAO) în conformitate cu forma și în ordinea stabilită de legislație și Procedura de redactare a materialelor privind contravențiile.
5.16. În cazul în care se dovedește că persoana care face obiectul inspecției a comis o contravenție prevăzută de articolul 188^{39} sau articolul 188^{40} din CUoAO în cursul inspecției, Comisarul sau funcționarul desemnat în conformitate cu articolul 255 partea 1 punctul 1 din CUoAO întocmește un proces verbal de contravenție în conformitate cu forma și în ordinea stabilită de legislație și Procedura de elaborare a materialelor privind contravențiile.
5.17. În cazul constatării unei infracțiuni în cursul inspecției asupra persoanei care face obiectul inspecției, Comisarul trimite materialele relevante autorităților judiciare.

6. Drepturile și obligațiile funcționarului desemnat și ale reprezentanților persoanei care face obiectul inspecției

6.1. Funcționarul desemnat în decursul inspecției are dreptul la:
6.1.1. Acces liber la obiectul inspecției la prezentarea legitimației de serviciu și acces liber la locurile de stocare a informațiilor, inclusiv computere, suporturi de date magnetice etc.

6.1.2. La cerere, acces la orice informații (documente) ale deținătorilor și administratorilor de date cu caracter personal necesare pentru a exercita controlul asupra respectării protecției datelor cu caracter personal, inclusiv accesul la datele cu caracter personal, bazele de date relevante sau fișetele cu fișiere, precum și la informații cu acces limitat.
În cazul în care documentul există numai în formă electronică, cu condiția ca acest document să fie creat de persoana care face obiectul inspecției, respectiva persoană este obligată să furnizeze copia pe suport de hârtie a acestui document, care asigură citirea sa vizuală, copie certificată de către persoana care face obiectul inspecției, în ordinea stabilită prin legislație. În cazul în care nu se furnizează copia pe suport de hârtie care asigură citirea sa vizuală, documentul electronic va fi revizuit, cu întocmirea Actului de revizuire a documentului electronic în conformitate cu Suplimentul 3 la prezenta Procedură.
6.1.3. Să primească copii ale documentelor certificate corespunzător în ordinea stabilită prin legislație.
6.1.4. Să ceară, în baza mandatului său, explicații scrise din partea conducătorului și/sau reprezentantului persoanei care face obiectul inspecției.
6.1.5. Să se adreseze organelor de urmărire penală și altor autorități de aplicare a legii în vederea îndeplinirii mandatului.
6.1.6. Să emită și să semneze Ordine de îmbunătățire privind prevenirea și eliminarea încălcărilor legislației privind protecția datelor cu caracter personal.
6.1.7. Să emită și să semneze procese verbale de contravenție pentru încălcarea legislației privind protecția datelor cu caracter personal.
6.1.8. Să ia legătura cu alte persoane prezente la momentul constatării contravenției, pentru încheierea procesului verbal.

6.2. La desfășurarea unei inspecții, funcționarul desemnat este obligat:
6.2.1. Să desfășoare inspecția în cadrul mandatului stabilit, pe deplin, în mod obiectiv și fără a fi părtinitor;
6.2.2. Să informeze conducătorul persoanei care face obiectul inspecției sau persoana desemnată cu privire la îndatoririle și mandatul funcționarului desemnat, motivul și scopul inspecției, drepturile, obligațiile conducătorului și ale reprezentanților persoanei care face obiectul inspecției;
6.2.3. Să informeze conducătorul persoanei care face obiectul inspecției sau persoana desemnată cu privire la rezultatele inspecției și/sau procesul verbal de contravenție;
6.2.4. Să definească lista de documente necesare de verificat și termenele de depunere a acestora;
6.2.5. Să formuleze rezultatele inspecțiilor în ordinea corespunzătoare;
6.2.6. Să respecte cu strictețe cerințele pentru întocmirea proceselor verbale stabilite prin Procedura de formulare a materialelor privind contravențiile.

6.3. Reprezentanții persoanei care face obiectul inspecției, inclusiv conducătorul persoanei care face obiectul inspecției sau persoana desemnată de acesta, la efectuarea inspecției, au dreptul:
6.3.1. Să verifice dacă funcționarul desemnat are legitimația de serviciu și temei de inspecție;
6.3.2. Să fie prezenți la desfășurarea inspecției;
6.3.3. Să primească și să cunoască rezultatele inspecției efectuate împreună cu Actul și/sau procesul verbal de contravenție;
6.3.4. Să furnizeze explicații și observații pe marginea Actului și/ sau procesului verbal de contravenție, în formă scrisă;
6.3.5. Să conteste acțiunile ilegale ale funcționarului desemnat în ordinea stabilită de legislație.

6.4. Reprezentanții persoanei care face obiectul inspecției, inclusiv conducătorul persoanei care face obiectul inspecției sau persoana desemnată, la efectuarea inspecției, au obligația:
6.4.1. Să asigure accesul liber al funcționarului desemnat la sediul persoanei care face obiectul inspecției și să ofere acces la documentele și alte materiale necesare desfășurării inspecției;
6.4.2. Să furnizeze documentele necesare și alte informații, explicații scrise confirmate prin semnătură, precum și alte copii ale documentelor necesare efectuării inspecției, certificate în ordinea stabilită de legislație.
6.4.3. Să respecte cerințele funcționarului/funcționarilor desemnați în ceea ce privește respectarea cerințelor legislației privind protecția datelor cu caracter personal.

Act de inspecție privind respectarea legislației privind protecția datelor cu caracter personal, adoptat de Comisarul Parlamentului Ucrainei pentru Drepturile Omului

«___» _____ 20__ _____
(ora și locul inspecției)

Subsemnatul/subsemnații,

_____
(funcția și numele persoanelor care desfășoară inspecția)

cu privire la

_____
(funcția și numele)

în prezența

_____
[funcția, numele și conducătorul persoanei juridice (funcționarul desemnat de aceasta) sau numele persoanei juridice - persoana care face obiectul inspecției]

Am desfășurat o inspecție

_____
(programată, neprogramată, în teren, neîntreruptă)

asupra respectării legislației privind protecția datelor cu caracter personal

_____
(denumirea, adresa persoanei juridice sau numele, domiciliul persoanei fizice - persoana care face obiectul inspecției)

Data începerii inspecției: «___» _____ 20___ anul ____ ora ____ minutul;

Data încheierii inspecției: «___» _____ 20___ anul ____ ora ____ minutul;

Durata totală a inspecției: ____ zile (___ ore ___ minute)

Ca urmare a inspecției, s-au constatat următoarele:

_____
_____
_____
_____
_____
_____
_____
_____
_____

Concluzii:

_____
(informații privind rezultatele inspecției, inclusiv abaterile constatate de la legea privind protecția datelor cu caracter personal)
_____
_____
_____

_____

_____

_____

_____

_____

_____

Observațiile persoanelor fizice sau juridice - persoana care face obiectul inspecției

_____

_____

_____

_____

_____

_____

Inspecția a fost desfășurată de:

_____	_____	_____
(funcția)	(semnătura)	(nume)
_____	_____	_____
(funcția)	(semnătura)	(nume)
_____	_____	_____
(funcția)	(semnătura)	(nume)

Actul inspecției a fost redactat în dublu exemplar:

Primul exemplar al actului se înmânează

_____

Al doilea exemplar al actului se înmânează

_____

Confirmarea Actului:

_____	_____	_____
(funcția)	(semnătura)	(nume)

Exemplarul Actului a fost primit de:

_____	_____	«___» _____ 20__
[funcția, numele și conducătorul persoanei juridice (funcționarul desemnat de acesta) sau numele persoanei juridice - persoana care face obiectul inspecției]	(semnătura)	

Anexa 3: Exercițiu de soluționare a cauzelor realizat de Centrul Național pentru Protecția Datelor cu Caracter Personal din Republica Moldova

Cauza privind dreptul de a fi uitat
pentru atelierul de soluționare a cauzelor

Realizat de Centrul Național pentru Protecția Datelor cu Caracter Personal din Republica Moldova

Circumstanțe

Reclamație împotriva unui blogger, pentru ștergerea informațiilor legate de solicitant de pe o pagină de web.

Postarea de pe blog a reflectat următoarele date cu caracter personal:
1) detalii privind o hotărâre judecătorească în care persoana a fost găsită vinovată de pedofilie,
2) informații privind viața sa profesională: că prestează lucrări de construcții prin societatea sa (fiind asociat unic și membru unic al consiliului de administrație) și că manopera este slabă (execută lucrări insuficiente - repară și construiește obiecte la un nivel scăzut de calitate).

Solicitantul a explicat că și-a îndeplinit condamnarea la închisoare (în urmă cu doi ani) și i-a fost greu să găsească clienți noi și o locuință datorită faptului că oamenii fac verificări pe internet.

De asemenea, acesta a explicat că observațiile privind manopera sa de slabă calitate au fost defăimătoare și au avut un impact negativ asupra sa.

1. Primirea reclamației, desemnarea responsabilului de caz:

1.1) Prin ce canale poate fi depusă o reclamație sau care sunt canalele cele mai frecvente? [prin poștă, poștă electronică, printr-o aplicație web, verbal]

MD
Prin poștă sau poșta electronică cu semnătură digitală.

1.2) Cum este desemnat responsabilul (final) de caz?

MD
De către Directorul Centrului și șeful subdiviziei

1.3) Verificările (formale și de fond) sunt efectuate de către un singur responsabil de caz sau sunt împărțite (dacă da, cum)?

MD
Nu

1.4) Cine semnează documentele în numele Autorității pentru Protecția Datelor în acest caz?

MD
Șeful subdiviziunii în care activează responsabilul de caz. Pentru decizii finale, persoana responsabilă este directorul centrului.

2. Termen limită

2.1) Care este termenul final obligatoriu pentru un caz bazat pe reclamație, (cum) poate fi acesta prelungit?

MD
30 de zile conform articolului 27 alineatul (3) din Legea nr. 133 privind protecția datelor cu caracter personal. Se poate prelungi, la cerere, cu câte 30 de zile.

2.2) Dacă există deficiențe care trebuie eliminate de către reclamant, cum afectează acestea termenul final?

MD
Procedură similară.

3. Verificări preliminare (inițiale)

3.1) Cum se procedează dacă reclamația nu este în limba oficială?

MD
Acceptăm, analizăm și răspundem conform cu Legea nr. 3465 privind limbile vorbite în teritoriu (în limba oficială a statului și în limba rusă).

3.2) Ce cerințe formale simple sunt verificate preliminar? Presupunem că:

- Numele, semnătura, data și informațiile de contact trebuie comunicate,
- Existența competenței juridice poate fi verificată preliminar (în cazul în care cauza intră sub incidența legislației de protecție a datelor și este de competența Autorității pentru Protecția Datelor)
- Adresa web exactă necesară în cazurile care prevăd dreptul de a fi uitat,
- Este totul corect? Mai este ceva?

MD
Dreptul de a fi uitat nu este transpus explicit în dreptul intern, dar tratăm extensiv dreptul de a contesta. Acestea sunt practic aceleași cerințe cu cele menționate mai sus și o verificare adițională dacă reclamația a fost făcută în termen de 30 de zile de la data faptelor.

3.3) Cum sunt cerute explicațiile părților asociate (în cazul nostru,deținătorul blogului și alte persoane care au avut postări pe blog)? Se va face în faza inițială? Cum le este verificată identitatea?

MD
În formă scrisă. Identitatea este verificată pe baza informațiilor comunicate de solicitant. Dacă este necesar, verificăm și informațiile de la sursele statului sau din alte mijloace disponibile. Acest pas nu este inclus în faza inițială.

3.4) Cât de repede trebuie efectuate verificările preliminare conform cu normele interne?

MD
În termen de 5-10 zile.

4. Verificări de fond - discreție și raționament

Aspecte de fond supuse analizei:

4.1) Avem un prag prevăzut prin dreptul privat aplicabil?
Trebuie făcută distincția între două aspecte ale reclamației (divulgarea cazierului judiciar, criticarea serviciului oferit) în contextul pragului de drept privat?

MD
În Moldova, publicarea hotărârilor judecătorești este reglementată de Legea nr. 514 din 6.7.1995, care prevede explicit la articolul 47. (3) punctul (e) că, înainte de publicare, hotărârile judecătorești sunt depersonalizate. În acest caz, însă, această prevedere nu este respectată și dacă sentința este publicată în forma sa completă fără a avea în vedere excepțiile Legii nr. 133 (precum interesul public), acest fapt este considerat o încălcare.

4.2) Dacă însă considerăm că acest caz este parțial sau complet peste pragul de drept privat, cum constatăm încălcarea drepturilor? În special în contextul conflictului dintre dreptul la viață privată/dreptul de a fi uitat și dreptul de a aminti/libertatea de expresie/libertatea de informare? Ce nivel de discreție avem - daune excesive, etică? Facem trimitere aici la dreptul internațional și constituțional?

MD
Articolul 5, , Articolul 10 și Articolul 16 din Legea nr. 133 sunt relevante pentru legislația relativă la accesul la informații, libertatea de expresie și alte legi care menționează explicit publicarea datelor cu caracter personal. În mod specific, articolul 5 alineatul (5) din Legea nr. 133 este relevant, acesta stipulând că nu este necesar consimțământul persoanei vizate dacă - se încheie un contract la care persoana vizată este parte - persoana împuternicită de către operator își îndeplinește o obligație conform legii - persoana vizată este protejată - există un interes public - datele sunt folosite în scopuri științifice, dacă se protejează anonimitatea persoanei vizate Da. Facem trimitere la dreptul internațional și constituțional.

4.3) Dacă considerăm că divulgarea cazierului judiciar este peste pragul prevăzut de dreptul privat, ce importanță au normele naționale privind expirarea cazierului judiciar?

MD
Prelucrarea datelor privind condamnările penale, măsurile procedurale de constrângere și infracțiunile poate fi efectuată doar de către sau sub controlul autorităților publice, în limitele competențelor acordate și în condițiile stabilite de lege [articolul 8 alineatul (1) din Legea nr. 133].

4.4) Care este concluzia - se intervine și se inițiază procedurile sau nu?

MD
Cu privire la acuzația de defăimare a firmei de construcții, Autoritatea de Protecție a Datelor nu este organul competent. Poliția este instituția responsabilă pentru astfel de capete de acuzare. În ceea ce privește publicarea hotărârii judecătorești asupra cazului de pedofilie, instanța trebuia să depersonalizeze publicarea pe site. În acest caz, pentru a nu afecta independența justiției, cererea este adresată inspectoratului judiciar. Cu toate acestea, instanța va comunica o evaluare a corectitudinii acțiunii de prelucrare a datelor cu caracter personal.

4.5) Dacă da, ce măsuri putem lua în acest caz?

MD
Depunerea materialelor cauzei la inspectoratul judiciar.

Anexa 4: Exemplu de cauză concretă soluționată de Comisariatul pentru Informații din Regatul Unit

Această cauză privește:
- corespondență de marketing nesolicitată;
- dreptul de a bloca prelucrarea pentru scopuri de marketing direct; și
- Serviciul de Preferințe Poștale.

Dna W a dorit ca o organizație de caritate să înceteze a-i trimite corespondență de marketing prin care se cereau donații.

Aceasta a scris organizației, atașând copii ale corespondenței nedorite, și a cerut încetarea trimiterii acestor materiale. Cu toate acestea, organizația de caritate a continuat să trimită corespondență de marketing, astfel încât dna W ne-a contactat.

Am sfătuit-o să scrie organizației și să întrebe de ce aceștia continuă să trimită materiale în scop de marketing și să le explice că în baza Legii privind protecția datelor, persoanele au dreptul să ceară organizațiilor să nu le folosească numele și adresa în scopuri de marketing.

De asemenea, am sfătuit-o să își înregistreze datele la Serviciul de Preferințe Poștale, care are în evidență o listă a persoanelor care nu doresc să primească corespondență de marketing adresată direct. Cu toate că organizațiile nu sunt obligate legal să verifice Serviciul de Preferințe Poștale înainte de a trimite material de marketing, majoritatea o fac.

Organizația de caritate a contactat-o pe dna W și și-a cerut scuze pentru inconvenientul cauzat. Aceștia i-au explicat că după ce au fost contactați prima dată de dânsa, i-au șters datele din lista de destinatari, ceea ce ar fi trebuie să rezolve problema. Cu toate acestea, ulterior aceștia au achiziționat o nouă listă de destinatari și nu au observat că numele acesteia se afla în listă, decât după primirea celei de-a doua scrisori.

Organizația de caritate a confirmat că va șterge din listele viitoare numele clienților care cer să nu fie contactați.