„Instruire orizontală în domeniul prelucrării datelor cu caracter personal pentru beneficiarii FESI”, cod proiect 1.1.114, cod SMIS2014+ 129690 proiect co-finanțat din Fondul European de Dezvoltare Regională prin Programul Operațional Asistență Tehnică (POAT) 2014-2020

CURS DE FORMARE PROFESIONALĂ SPECIALIZATĂ ŞI CERTIFICATĂ ANC ÎN DOMENIUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

AGENȚIA NAȚIONALĂ A FUNCȚIONARILOR PUBLICI

Acest material a fost realizat astfel:

Capitolul		Autorul
I.	*Noțiuni introductive cu privire la domeniul protecției datelor cu caracter personal, la drepturile și obligațiile instituțiilor și ale persoanelor implicate în prelucrarea datelor cu caracter personal. Principii privind prelucrarea datelor cu caracter personal*	Prof.univ.dr.Fuerea Augustin, Dr.Păcurar Gheorghe
II.	*Identificarea modalităților și instrumentelor de monitorizare a modului în care instituția /autoritatea respecta prevederile în domeniul prelucrării datelor cu caracter personal, organizarea și utilizarea acestora în cadrul instituției/autorități*	Dr.Katona Levente
III.	*Sfera activităților aferente asistenței de specialitate acordate de responsabilul pentru protecția datelor cu caracter personal, elaborarea planului de lucru al acestuia și proceduri de lucru eficiente care să sprijine DPO în exercitarea atribuțiilor*	Prof.univ.dr.Rădulescu Dragoș
IV.	*Relația cu autoritatea de supraveghere în domeniul protecției datelor cu caracter personal și rolul punctului de contact*	Av.dr.Radu Daniela
V.	*Aspecte specifice cu privire la rolul si activitatea responsabilului pentru protecția datelor cu caracter personal*	Prof.univ.dr.Mureșan Mihaela
VI.	*Metodologii de evaluare a impactului asupra protecției datelor (DPIA) și stabilirea dacă o prelucrare este "susceptibilă să genereze un risc ridicat"*	Ec.Mureșan Liviu

C U P R I N S

CAP. I. NOȚIUNI INTRODUCTIVE CU PRIVIRE LA DOMENIUL PROTECȚIEI DATELOR CU CARACTER PERSONAL, LA DREPTURILE ȘI OBLIGAȚIILE INSTITUȚIILOR ȘI ALE PERSOANELOR IMPLICATE ÎN PRELUCRAREA DATELOR CU CARACTER PERSONAL. PRINCIPII PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL.

Noțiuni introductive cu privire la domeniul protecției datelor cu caracter personal

Aspecte generale privind drepturile și obligațiile instituțiilor și ale persoanelor implicate în prelucrarea datelor cu caracter personal

Principii privind prelucrarea datelor cu caracter personal

Noțiuni introductive cu privire la domeniul protecției datelor cu caracter personal

Analizând problematica protecției datelor care au caracter personal este cu neputință să nu observăm multe dintre trăsăturile care îi aparțin și pe care le întâlnim și în alte domenii, dar și caracteristicile care îi sunt proprii, particularizând-o atunci când o raportăm la alte materii. Între acele trăsături care îi aparțin, dar pe care le întâlnim și în alte domenii, se remarcă vastitatea acestei problematici, dinamica (internă, europeană și internațională), dar și complexitatea determinată, între altele, de numeroase interferențe interdisciplinare.

1. Instrumente juridice internaționale care conțin prevederi consacrate protecției datelor cu caracter personal

A. Declarația Universală a Drepturilor Omului

Încă din anul 1948, la nivel internațional, sub auspiciile Organizației Națiunilor Unite, au fost adoptate norme dedicate protecției unor date cu caracter personal. În acest sens, menționăm Declarația Universală a Drepturilor Omului care, la art. 12, dispune faptul că „nimeni nu va fi supus la imixtiuni arbitrare în viaţa sa personală, în familia sa, în domiciliul lui sau în corespondenţa sa, nici la atingeri aduse onoarei şireputaţiei sale”. Acestor mențiuni i se adaugă și cea potrivit căreia„orice persoană are dreptul la protecţia legii împotriva unor asemenea imixtiuni sau atingeri.

B. Convenția Europeană a Drepturilor Omului

Un alt instrument juridic internațional, de data aceasta având forță juridică obligatorie, este Convenția pentru Apărarea Drepturilor Omului și a Libertăților Fundamentale, cunoscută și sub denumirea de Convenția Europeană a Drepturilor Omului. Adoptată la nivelul Consiliul Europei, Convenția consacră, la art. 8, dreptul persoanelor la respectarea vieţii private şi de familie. În acest sens, alin. (1) al art. 8 prevede că „orice persoană are dreptul la respectarea vieţii sale private şi de familie, a

domiciliului său şi a corespondenţei sale". Alineatul (2) completează această dispoziție, menționând că „nu este admis amestecul unei autorităţi publice în exercitarea acestui drept decât în măsura în care acesta este prevăzut de lege şi constituie, într-o societate democratică, o măsură necesară pentru securitatea naţională, siguranţa publică, bunăstarea economică a ţării, apărarea ordinii şi prevenirea faptelor penale, protecţiasănătăţii, a moralei, a drepturilor şi a libertăţilor altora".

C. Convenţia pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981[1]

Potrivit art. 1 al Convenției, scopul acesteia este acela „de a garanta, pe teritoriul fiecărui stat parte, fiecărei persoane fizice, oricare ar fi cetăţenia sa sau reşedinţa sa, respectarea drepturilor şilibertăţilor sale fundamentale şi, în special, dreptul la viaţa privată, faţă de prelucrarea automatizată a datelor cu caracter personal care o privesc (protecţia datelor)". În sensul Convenției, „datele cu caracter personal care fac obiectul unei prelucrări automatizate trebuie să fie: obţinuteşi prelucrate în mod corect şi legal; înregistrate în scopuri determinate şi legitime şi nu sunt utilizate în mod incompatibil cu aceste scopuri; adecvate, pertinente şi neexcesive în raport cu scopurile pentru care sunt înregistrate; exacte şi, dacă este necesar, actualizate; păstrate într-o formă care să permită identificarea persoanelor în cauză pe o durată ce nu o depăşeşte pe cea necesară scopurilor pentru care ele sunt înregistrate"[2]. În concordanță cu prevederile Convenției, „date cu caracter personal reprezintă orice informație privind persoana fizică identificată sau identificabilă (persoană vizată)"[3].

2. Temeiul legal al adoptării Regulamentului (UE) 2016/679

A. Tratatul privind funcționarea Uniunii Europene

Relevant pentru demersul nostru este art. 16 alin. (1) TFUE, potrivit căruia „orice persoană are dreptul la protecția datelor cu caracter personal care o privesc". În continuare, alin. (2) al aceluiași articol stabilește faptul că „normele privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii, precum și de către statele membre în exercitarea activităților care fac parte din domeniul de aplicare a dreptului Uniunii, precum și normele privind libera circulație a acestor date trebuie respectate. Respectarea acestor norme face obiectul controlului unor autorități independente".

TFUE precizează că art. 16 nu îndreptățește legislativul Uniunii Europene să adopte norme care să aducă atingere prevederilor specifice prevăzute la art. 39 TUE, adică, prin derogare, „Consiliul adoptă o decizie de stabilire a normelor privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către statele membre, în exercitarea activităților care fac parte din domeniul de aplicare (...), precum și a normelor privind libera circulație a acestor date". Același art.

[1] Ratificată de România prin Legea nr. 682/2001, publicată în Monitorul Oficial al României, Partea I, nr. 830 din 21 decembrie 2001.
[2] Art. 5 din Convenție.
[3] Art. 2 lit. a).

39 TUE, similar art. 16 TFUE, precizează că „respectarea acestor norme face obiectul controlului unor autorități independente”[4].

B. Tratatul privind Uniunea Europeană

Deși nu este menționat în mod special în referirile Regulamentului (UE) 2016/679, Tratatul privind Uniunea Europeană conține detalii cu privire la protecția datelor cu caracter personal. astfel, la art. 39, Tratatul prevede faptul că „în conformitate cu art. 16 TFUE și prin derogare de la alin. (2) al acestuia, Consiliul adoptă o decizie de stabilire a normelor privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către statele membre, în exercitarea activităților care fac parte din domeniul de aplicare, precum și a normelor privind libera circulație a acestor date. Respectarea acestor norme face obiectul controlului unor autorități independente”.

C. Carta Drepturilor Fundamentale a Uniunii Europene (denumită, în continuare, Carta), la art. 8 alin. (1), articol care este situat în Titlul al II-lea, denumit „Libertățile”, face precizarea potrivit căreia „orice persoană are dreptul la protecția datelor cu caracter personal care o privesc”, precizare identică celei pe care am remarcat-o la art. 16 alin. (1) TFUE. La cel de-al doilea alineat al art. 8, Carta adaugă prevederi care dau conținut și sens unui astfel de drept, deoarece „asemenea date trebuie tratate în mod corect, în scopurile precizate și pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege”. Mai mult, „orice persoană are dreptul de acces la datele colectate care o privesc, precum și dreptul de a obține rectificarea acestora”. Responsabilitatea respectării acestor norme este plasată tot sub controlul unei autorități independente. Nu întâmplător articolele (6 și 7) cu care debutează titlul al II-lea se referă la dreptul la libertate și siguranță (art. 6), respectiv la respectarea vieții private și de familie (art. 7), datele cu caracter personal având conotații relevante asupra celor două aspecte evidențiate, și nu numai.

3. Contextul adoptării Regulamentului (UE) 2016/679

„Abrogarea Directivei 95/46/CE[5], directivă care a urmărit armonizarea nivelurilor de protecție a drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește activitățile de prelucrare și asigurare a liberei circulații a datelor cu caracter personal între statele membre, vine în condițiile în care asistăm la evoluții tehnologice dintre cele mai rapide la care se adaugă tendințele de globalizare, aspecte ce conferă o amploare fără precedent colectării și schimbului de date cu caracter personal. Binomul „libertăți” și „protecție” trebuie să funcționeze coexistând mai departe. Coexistența se referă la facilitarea, în continuare, a libertății de circulație a datelor cu caracter personal în cadrul Uniunii și la transferul către țări terțe și organizații internaționale,

[4] La nivel național, există, în fiecare stat membru, câte o astfel de autoritate. În România își desfășoară activitatea Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal. La nivelul Uniunii Europene, există Comitetul european pentru protecția datelor, ca organ cu personalitate juridică, alcătuit, potrivit art. 68 alin. (3) din Regulament, „din șeful unei autorități de supraveghere din fiecare stat membru și din Autoritatea Europeană pentru Protecția Datelor sau reprezentanții respectivi ai acestora”

[5] Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, publicată în JO L 281, din 23.11.1995.

dar în condițiile în care se asigură și un nivel ridicat de protecție a datelor cu caracter personal”[6].

„Regulamentul a fost adoptat și cu luarea în considerare a unor dezavantaje pe care le-a dovedit Directiva 95/46/CE, dezavantaje specifice, de altfel, unui act juridic al UE de un astfel de tip, luat prin comparație cu cel de tipul regulamentului. Reține aici atenția faptul că directiva în discuție nu a reușit să prevină fragmentarea modului în care protecția datelor a fost asigurată în toate statele membre ale Uniunii Europene. Insecuritatea juridică sau percepția publică potrivit căreia există riscuri semnificative pentru protecția persoanelor fizice, în special referitoare la activitatea online, a fost larg răspândită. Se adaugă, din aceeași perspectivă a dezavantajelor directivei, faptul că diferențele dintre nivelurile de protecție existente în cele 27 de state membre ale UE, diferențe date de transpunerea și aplicarea directivei, au condus, uneori, la încetinirea punerii în aplicare a principiului libertății de circulație a datelor cu caracter personal, în cadrul UE, putându-se constitui în reale obstacole în desfășurarea activității economice la acest nivel, denaturând concurența și împiedicând autoritățile să-și îndeplinească responsabilitățile care le revin, potrivit dreptului UE”[7].

4. Temeiul legal intern al aplicării, cu prioritate, a dreptului internațional și a dreptului Uniunii Europene

A. Constituția României, republicată

- art. 20 alin. (2): „dacă există neconcordanţe între pactele şi tratatele privitoare la drepturile fundamentale ale omului, la care România este parte, şi legile interne, au prioritate reglementările internaţionale, cu excepţia cazului în care Constituţia sau legile interne conţindispoziţii mai favorabile[8]” (de ex.: Declarația Universală a Drepturilor Omului și Convenția pentru Apărarea Drepturilor Omului și a Libertăților Fundamentale);

- art. 148 alin. (2) și (4)[9] din Legea fundamentală: „ca urmare a aderării, prevederile tratatelor constitutive ale Uniunii Europene, precum şi celelalte reglementări comunitare cu caracter obligatoriu, au prioritate faţă de dispoziţiile contrare din legile interne, cu respectarea prevederilor actului de aderare[10]” (de ex.: Regulamentul (UE) 2016/679); „Parlamentul, Preşedintele României, Guvernul şi autoritatea judecătorească garantează aducerea la îndeplinire a obligaţiilor rezultate din actul aderării şi din prevederile” anterior menționate.

B. Codul civil conține, la art. 4 alin. (2) și art. 5, prevederi incidente materiei, după cum urmează: „dacă există neconcordanţe între pactele şi tratatele privitoare la drepturile fundamentale ale omului, la care România este parte, şi prezentul cod, au prioritate reglementările internaţionale, cu excepţia cazului în care prezentul cod conţinedispoziţii mai favorabile”, respectiv „în materiile reglementate de prezentul cod, normele dreptului Uniunii Europene se aplică în mod prioritar, indiferent de calitatea sau statutul părţilor”.

---

[6] **Augustin Fuerea**, *Aplicarea dreptului Uniunii Europene potrivit prevederilor Constituției României și ale altor norme de drept intern,* Revista Dreptul, nr. 6/2019, pag. 149-171.
[7] ***Idem***.
[8] Sublinierea noastră.
[9] Pentru un comentariu al art. 148, a se vedea **Roxana-Mariana Popescu,***Aspecte constituționale ale integrării României în Uniunea Europeană*, Revista Dreptul, nr. 3/2017, pag. 131-140.
[10] ***Idem***.

C. Codul de procedură civilă reglementează problema aplicării prioritare a normelor internaționale, în general, și a celor unionale, în special, astfel: „Dacă există neconcordanțe între pactele și tratatele privitoare la drepturile fundamentale ale omului, la care România este parte, și prezentul cod, au prioritate reglementările internaționale, cu excepția cazului în care prezentul cod conține dispoziții mai favorabile”[11] și „în materiile reglementate de prezentul cod, normele obligatorii ale dreptului Uniunii Europene se aplică în mod prioritar, indiferent de calitatea sau de statutul părților”[12];„Este necesară cunoașterea și aplicarea acestei legislații și a ordinii de prioritate atât în raporturile cu terții, cât și în cele care se stabilesc cu angajații proprii, tocmai pentru a preveni abuzurile la care s-ar putea ajunge din partea tuturor părților aflate în astfel de raporturi”[13].

5. Definiții

Regulamentul (UE) 2016/679, la art. 4 definește un număr de 26 concepte, dintre care le amintim pe următoarele:

A. „*date cu caracter personal*” înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

B. „*prelucrare*” înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

C. „*restricționarea prelucrării*” înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

D. „*pseudonimizare*” înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;

E. „*operator*” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile

[11] Art. 3 alin. (2).
[12] Art. 4.
[13] **Augustin Fuerea**, *Aplicarea legislației, în materia protecției datelor cu caracter personal, de către practicienii în insolvență*, Revista Universul Juridic, nr. 12/2020, pag. 113.

specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;

F. „*persoană împuternicită de operator*” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

G. „*consimțământ*” al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

H. „*prelucrare transfrontalieră*” înseamnă:

(a) fie prelucrarea datelor cu caracter personal care are loc în contextul activităților sediilor din mai multe state membre ale unui operator sau ale unei persoane împuternicite de operator pe teritoriul Uniunii, dacă operatorul sau persoana împuternicită de operator are sedii în cel puțin două state membre; sau

(b) fie prelucrarea datelor cu caracter personal care are loc în contextul activităților unui singur sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, dar care afectează în mod semnificativ sau este susceptibilă de a afecta în mod semnificativ persoane vizate din cel puțin două state membre.

6. Categorii de date cu caracter personal

„Datele cu caracter personal includ orice informații despre o persoană identificată sau identificabilă (**subiectul datelor**). Printre datele cu caracter personal se numără:

- numele;
- adresa;
- numărul cărții de identitate/pașaportului;
- venitul;
- profilul cultural;
- adresa IP (Internet Protocol);
- datele deținute de medici sau spitale (care identifică o persoană în scopuri medicale)”[14].

Acestora li se adaugă[15]: numărul de telefon, adresa electronică, datele de localizare, starea civilă, fotografia feței, obiceiurile și preferințele, identificatorii online și orice alte date ce țin de identitatea fizică, fiziologică, economică, culturală sau socială care pot utilizate pentru identificarea directă sau indirectă a unei persoane fizice.

Exemple:

- *„Obiceiuri şi practici profesionale informaţiile legate de prescripţia medicamentelor (de exemplu, număr de identificare al medicamentului, denumirea acestuia, tăria medicamentului, producătorul, preţul de vânzare, faptul dacă acesta este nou sau de rezervă, condiţiile de utilizare, condiţiile de înlocuire a acestuia,*

[14] https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_ro.htm (accesat la 18 aprilie 2021).

[15] Potrivit http://datepersonale.md/wp-content/uploads/2019/12/InfoPage_facts-to-be-known-final111.pdf (accesat la 18 aprilie 2021).

prenumele și numele persoanei care l-a prescris, numărul de telefon etc.), fie sub formă de prescripție separată sau sub formă de modele extrase dintr-o serie de prescripții, pot fi considerate drept date cu caracter personal referitoare la un medic care prescrie medicamentul, chiar dacă pacientul este anonim. Astfel, furnizarea de informații referitoare la prescripțiile scrise de medici identificați sau identificabili producătorilor de medicamente eliberate pe bază de rețetă reprezintă o comunicare a datelor cu caracter personal către destinatari terți"[16].

- *„serviciile bancare prin telefon: În cazul serviciilor bancare prin telefon, atunci când vocea clientului care oferă instrucțiuni băncii este înregistrată, instrucțiunile respective înregistrate trebuie considerate ca date cu caracter personal"*[17].

- *„supravegherea video: Imaginile referitoare la persoane capturate prin sisteme de supraveghere video pot constitui date cu caracter personal în măsura în care persoanele pot fi recunoscute"*[18].

- *„desenul unui copil: Ca urmare a unui test neuro-psihiatric efectuat pentru o fetiță în contextul unei acțiuni în justiție referitoare la custodia acesteia, este prezentat un desen realizat de fetița respectivă care prezintă familia acesteia. Desenul furnizează informații cu privire la starea fetițeișisi cu privire la sentimentele acesteia față de diverși membri ai familiei. Astfel, desenul poate fi considerat drept „date cu caracter personal". Acesta furnizează, într-adevăr, informații referitoare la copil (starea de sănătate a acestuia din punct de vedere psihic), precum și informații referitoare la, de exemplu, comportamentul tatălui sau al mamei acestuia. În consecință, în cauza respectivă, părințiiîși pot exercita dreptul de acces la această informație specifică"*[19].

Categorii speciale de date

„Articolul 37 alineatul (1) litera (c) Din Regulamentul (UE) 2016/679 se referă la prelucrarea unor categorii speciale de date prevăzute la art. 9 și la date cu caracter personal privind condamnări penale și infracțiuni prevăzute la art. 10. Deși în dispoziție este utilizat termenul „și", nu există niciun motiv pentru care să se impună aplicarea simultană a celor două criterii. Prin urmare, textul ar trebui să fie interpretat ca însemnând „sau"[20].

7. Date cu caracter personal pe timp de pandemie

Situația sanitară existentă în prezent la nivel internațional, are o serie de consecințe asupra aplicării Regulamentului (UE) 2016/679.

Regulamentul prevede norme speciale pentru prelucrarea datelor privind sănătatea în scopul cercetării științifice care sunt aplicabile și în contextul pandemiei de COVID-19. Potrivit art. 4 pct. 15 din Regulament, „date privind sănătatea" înseamnă „date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia". În concordanță cu considerentul 53 din preambulul Regulamentului, „datele privind sănătatea necesită un nivel mai ridicat de

[16] Exemplu preluat din *Avizul 4/2007 privind conceptul de date cu caracter personal*, adoptat la 20 iunie 2007, 01248/07/RO, WP 136, pag. 7.
[17] ***Ibidem***, pag. 9.
[18] ***Idem***.
[19] ***Idem***.
[20] Potrivit *Orientări privind responsabilii cu protecția datelor („RPD")*, adoptate la 13 decembrie 2016, astfel cum au fost recent revizuite și adoptate la 5 aprilie 2017, 16/RO GL 243 rev. 01, pag. 11.

protecție, deoarece utilizarea unor astfel de date sensibile poate avea efecte negative semnificative asupra persoanelor vizate. Având în vedere acest aspect, termenul „date privind sănătatea" trebuie interpretat în sens larg"[21].

„Datele privind sănătatea pot fi extrase din surse diferite, de exemplu:

- informații colectate de un furnizor de servicii medicale într-un dosar medical (cum ar fi antecedentele patologice și rezultatele examinărilor și tratamentelor);

- informații care devin date privind sănătatea prin trimiteri încrucișate la alte date ce indică starea de sănătate sau riscurile privind sănătatea (cum ar fi ipoteza că o persoană are un risc mai mare de a suferi un atac cardiac pe baza valorilor mai mari ale tensiunii arteriale măsurate într-o anumită perioadă de timp);

- informații dintr-un chestionar de autoevaluare, în care persoanele vizate răspund la întrebări legate de sănătatea lor (cum ar fi enumerarea simptomelor);

- informații care devin date privind sănătatea ca urmare a utilizării lor într-un anumit context (cum ar fi informații despre o deplasare recentă sau despre prezența într-o regiune afectată de COVID-19, prelucrate de un cadru medical în vederea stabilirii unui diagnostic)"[22].

Prelucrările de date cu caracter personal privind sănătatea trebuie să respecte prevederile art. 5 din Regulament, dar și derogările specifice enumerate la art. 6 și 9 din Regulament.

„Legiuitorul național al fiecărui stat membru poate adopta prevederi specifice în temeiul art. (9) alin. (2) lit. (i) și (j) din Regulament pentru a permite prelucrarea datelor privind sănătatea în scopuri de cercetare științifică. Prelucrarea datelor privind sănătatea în scopul cercetării științifice trebuie, de asemenea, să fie acoperită de unul dintre temeiurile juridice prevăzute la art. 6 alin. (1) din Regulament. Prin urmare, condițiile și amploarea unei astfel de prelucrări variază în funcție de legislația adoptată de statul membru respectiv"[23].

„Având în vedere riscurile de prelucrare în contextul pandemiei de COVID-19, trebuie să se pună un accent deosebit pe respectarea art. 5 alin. (1) lit. (f), a art. 32 alin. (1) și a art. 89 alin. (1) din Regulament. Trebuie să se evalueze dacă este necesară o evaluare a impactului asupra protecției datelor în temeiul art. 35 din Regulament"[24].

„În principiu, situațiile precum actuala pandemie de COVID-19 nu suspendă și nu restricționează posibilitatea ca persoanele vizate să își exercite drepturile în temeiul art. 12-22 din Regulament. Cu toate acestea, art. 89 alin. (2) permite legiuitorului național să restricționeze (unele) drepturi ale persoanei vizate, astfel cum se prevede în capitolul III din Regulament. Din acest motiv, restricțiile privind drepturile persoanelor vizate pot varia în funcție de legislația adoptată de statul membru respectiv"[25].

8. Exemple din practica instanțelor

A. Curtea de Justiție a Uniunii Europene

a.„Hotărârea Curții de Justiție a Uniunii Europene, potrivit căreia, începând cu data de 1 iulie 2018, cauzele preliminare care implică persoane fizice vor fi anonimizate[26]. Decizia CJUE a fost luată „în contextul în care (…) noul Regulament

[21] Comitetul European Pentru Protecția Datelor, *Orientările 3/2020 referitoare la prelucrarea datelor privind sănătatea în scopul cercetării științifice în contextul pandemiei de COVID-19*, adoptate la 21 aprilie 2020, pag. 5.
[22] ***Idem***.
[23] ***Ibidem,*** pag. 14.
[24] ***Ibidem,*** pag. 15.
[25] ***Idem***.
[26] Conform *Comunicatului de presă nr. 96/18* (din 29 iunie 2018) al CJUE.

general privind protecția datelor [RGPD] a intrat în vigoare”[27] și se aplică „precedându-l pe cel care va fi în curând aplicabil instituțiilor UE”[28]. Scopul deciziei CJUE este acela de a consolida „protecția datelor persoanelor fizice în cadrul publicațiilor privitoare la cauzele preliminare”. (...) Contextul este motivat de diversificarea, respectiv de „multiplicarea mijloacelor de căutare și de difuzare” a datelor cu caracter personal. În mod concret, Curtea de decis faptul că „pentru orice cauză preliminară introdusă începând cu 1 iulie 2018, [se vor înlocui] cu inițiale, în toate documentele sale publicate [numele] persoanelor fizice implicate în cauză”. De asemenea, potrivit aceleiași decizii, va fi înlăturată orice informație care ar fi de natură să permită identificarea (și, adăugăm noi, potrivit art. 4 pct. 1 din Regulament, identificabilitatea) persoanelor în cauză[29]„[30].

b.„Hotărârea Curții de Justiție a Uniunii Europene pronunțată în cauza ***Novak***[31], potrivit căreia „răspunsurile scrise furnizate în cadrul unui examen profesional și eventualele observații ale examinatorului referitoare la aceste răspunsuri constituie date cu caracter personal ale candidatului la care are, în principiu, un drept de acces”[32]. Accesul candidatului la astfel de informații răspunde obiectivului urmărit de legislația UE care se referă la protecția dreptului la viața privată a persoanelor fizice privind prelucrarea datelor acestora, potrivit aceluiași comunicat. În anul 2017, nu se aplicau prevederile Regulamentului (UE) 2016/679, ci acelea ale Directivei 95/46[33], directivă potrivit căreia datele cu caracter personal reunesc „orice informație referitoare la o persoană fizică identificată sau identificabilă”[34]”[35].

c. Hotărârea Curții de Justiție a Uniunii Europene „pronunțată în cauza ***C-25/17***[36], potrivit căreia „o comunitate religioasă, (...), este operator[37], împreună cu membrii săi predicatori, în ceea ce privește prelucrarea datelor cu caracter personal colectate în cadrul unei activități de predicare din casă în casă”[38] și, pe cale de consecință, o astfel de activitate trebuie să respecte legislația UE cu privire la protecția datelor cu caracter personal. Aceste date se referă, potrivit hotărârii CJUE, la numele și adresele persoanelor vizate, convingerile religioase ori la situația lor familială. Prin urmare, activitatea membrilor comunității în cauză nu intră sub incidența excepțiilor prevăzute

---

[27] ***Idem***.

[28] La acea dată aplicându-se Regulamentul (CE) nr. 45/2001 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date, publicat în JO L8, 12.1.2001, abrogat prin Regulamentul (UE) 2018/1725 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date (publicat în JO L 295, 21.11.2018).

[29] Pentru detalii tehnice (inițiale ș.a.), a se vedea Comunicatul invocat.

[30] **Augustin Fuerea**, *Aplicarea legislației, în materia..., op. cit.*, pag. 116.

[31] Hotărârea Curții din 20 decembrie 2017, *Peter Nowak c./ Data Protection Commissioner*, C-434/16, EU:C:2017:994.

[32] Pct. 27 din hotărâre.

[33] Directiva 95/46/CE, *precitată*.

[34] Pct. 28 din hotărârea *Novak*. În prezent, la art. 4 pct. 1 se precizează că „o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale”.

[35] **Augustin Fuerea**, *Aplicarea legislației, în materia..., op. cit.*, pag. 116-117.

[36] Hotărârea Curții din 10 iulie 2018, *Tietosuojavaltuutettu*, C-25/17, EU:C:2018:551.

[37] Operator de date cu caracter personal este „persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern” (potrivit art. 4 pct. 7 din Regulamentul (UE) 2016/679).

[38] Potrivit pct. 75 din hotărârea pronunțată în cauza C-25/17, *precitată*.

de dreptul UE în materie". Mai exact, instanța precizează că această activitate de predicare din casă în casă, prin colectarea mai multor date personale „nu este o activitate exclusiv personală sau domestică"[39] cu privire la care dreptul UE nu s-ar aplica"[40].

B. Curtea Europeană a Drepturilor Omului

a.Hotărârea Curții Europene a Drepturilor Omului pronunțată în cauză *Bărbulescu c./România*[41]. „Cauza „privește decizia unei societăți civile de a concedia un angajat – reclamantul – după monitorizarea comunicațiilor sale electronice și a conținutului acestora. Reclamantul a arătat faptul că decizia angajatorului său se întemeia pe o încălcare a vieții sale private și a corespondenței"[42]. Hotărârea dată de Marea Cameră (cu 11 voturi pentru și 1 împotrivă) a fost în sensul că angajatorul a încălcat art. 8 din Convenție, iar „autoritățile române nu au protejat, în mod corespunzător, dreptul reclamantului la respectarea vieții private și a corespondenței". Mai mult, instanțele române nu au reușit să constate dacă angajatorul și-a îndeplinit o obligație (pe care și Regulamentul o prevede la art. 13 și 14), și anume aceea de a fi informat reclamantul asupra acestei măsuri, anterior instituirii monitorizării"[43].

b.Hotărârea Curții Europene a Drepturilor Omului„pronunțată în cauza *Libert c./Franța*[44]. Plângerea reclamantului a vizat încălcarea dreptului său la respectarea vieții private de către angajatorul său care a deschis fișiere aflate în partiția sa de pe hard-diskul calculatorului pe care lucra în interes de serviciu, intitulată „D:/date personale" în condițiile în care angajatul nu a fost invitat să asiste la operațiune. Dat fiind conținutul fișierelor deschise, în situația mai sus arătată, angajatul a fost demis. În temeiul art. 8 din Convenție, Curtea a comunicat cererea guvernului francez și a adresat întrebări părților"[45].

c.Alte cauze ale Curții Europene a Drepturilor Omului, relevante pentru domeniu, vizează: stocarea și utilizarea datelor cu caracter personal în contextul sistemului de justiție penală[46], în contextul sănătății[47], în procedurile din domeniul asigurărilor sociale[48], în stocarea datelor în registre secrete[49], date ale furnizorilor de servicii de telecomunicații, divulgarea datelor cu caracter personal[50], accesul la date cu caracter personal[51], ștergerea sau distrugerea datelor cu caracter personal[52]"[53].

---

[39]***Ibidem***, pct. 42.
[40]**Augustin Fuerea**, *Aplicarea legislației, în materia..., op. cit.*, pag. 117.
[41] Hotărârea din 5 septembrie 2017, cererea 61496/08.
[42]https://www.echr.coe.int/Documents/FS_Data_RON.pdf, accesat la 16 ianuarie 2020.
[43]**Augustin Fuerea**, *Aplicarea legislației, în materia..., op. cit.*, pag. 118.
[44] Hotărârea din 2 iulie 2018 (cererea 588/13).
[45]**Augustin Fuerea**, *Aplicarea legislației, în materia..., op. cit.*, pag. 118.
[46]*Perry c./ Regatul Unit* (hotărârea din 17 iulie 2003, cererea 63737/00); *S și Marper c./Regatul Unit* (hotărârea din 4 decembrie 2008, cererile nr. 30562/04 și 30566/04); *Uzun c./Germania* (hotărârea din 2 septembrie 2010, cererea 35623/05); *Dimitrov-Kazakov c./Bulgaria* (hotărârea din 10 februarie 2011, cererea 11379/03); *Brunet c./Franța* (hotărârea din 18 septembrie 2014, cererea 21010/10) ș.a.
[47]*Chave născută Jullien c./Franța* (hotărârea din 9 iulie 1991, cererea 14461/88) ș.a.
[48]*Vukota c./Elveția* (hotărârea din 18 octombrie 2016, cererea 61838/10) ș.a.
[49]*Rotaru c/România* (hotărârea din 4 mai 2000, Marea Cameră, cererea 28341/95); Turek c./Slovacia (hotărârea din 14 februarie 2006, cererea 57986/00) ș.a.
[50]*Radu c./Republica Moldova* (hotărârea din 15 aprilie 2014, cererea 50073/07) ș.a.
[51]*Haralambie c./România* (hotărârea din 27 octombrie 2009, cererea 21737/03); *Jarnea c./România* (hotărârea din 19 iulie 2011, cererile 36268/02, 25416/04, 25500/04, 43454/06, 24717/07, 16297/08 și 17068/08); *Antoneta Tudor c./România* (hotărârea din 24 septembrie 2013, cererea 23445/04) ș.a.
[52]*Rotaru c./România, precitată*; *Asociația 21 Decembrie 1989 ș.a. c./România* (hotărârea din 24 mai 2011, cererile 33810/07 și 18817/08) ș.a.
[53]**Augustin Fuerea**, *Aplicarea legislației, în materia..., op. cit.*, pag. 118-119.

C. Instanțe din România

a. „Tribunalul București a sesizat CJUE[54] pentru a se edifica asupra condițiilor care „trebuie îndeplinite pentru a se putea aprecia că o manifestare de voință este una specifică și informată în conformitate cu legislația UE”[55]. O astfel de sesizare a intervenit în condițiile în care Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, în urma unei anchete desfășurate la sediile Orange din București (Orange fiind operator de date cu caracter personal), la data de 26 martie 2018, a descoperit copii ale actelor de identitate[56] ale clienților săi. Pe cale de consecință, Autoritatea i-a aplicat Orange o amendă administrativă. Temeiul invocat în raportul de anchetă a fost, la aceea dată, Legea nr. 677/2001 cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date[57] (art. 8 și 32). În verificarea pe care Autoritatea a realizat-o a urmărit, inclusiv, aplicarea Legii nr. 506/2004 privind prelucrarea rapidă a datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice[58]. Starea de fapt se referă la situația în care se găsește Orange, ca furnizor de servicii de telecomunicații mobile pe piața din România, inclusiv în sistemul „PrePay”, iar colectarea datelor cu caracter personal îi vizează pe clienții săi. Aceștia încheiau contracte de servicii având posibilitatea de a achiziționa echipamente în condiții avantajoase, beneficiind de reduceri de preț, facilități la transfer și altele”[59].

b. Tribunalul București a solicitat Curții de Justiție a UE interpretarea dreptului Uniunii[60] aplicabil în materia protecției datelor cu caracter personal, cu trimitere directă la păstrarea confidențialității în materia datelor cu caracter personal de către o asociație de proprietari, în calitate de pârâtă.

9. Legislație specifică domeniului protecției datelor cu caracter personal

A. Norma-cadru în domeniu, la nivelul Uniunii Europene

⇨ Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor).

---

[54] *Orange Romania SA c. / Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*, C-61/19, EU:C:2020:901.

[55] Potrivit http://curia.europa.eu/juris/showPdf.jsf?text=&docid=219794&pageIndex=0&doclang=RO&mode=lst&dir=&occ=first&part=1&cid=1232077, accesat la 20 ianuarie 2020).

[56] Aceste copii au fost luate și păstrate fără acordul expres al clienților Orange.

[57] În prezent este aplicabilă Legea nr. 129/2018 pentru modificarea și completarea Legii nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum și pentru abrogarea Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, publicată în Monitorul Oficial al României, Partea I, nr. 503 din 19 iunie 2018.

[58] Publicată în Monitorul Oficial al României, Partea I, nr. 1101/2004.

[59] **Augustin Fuerea**, *Aplicarea legislației, în materia..., op. cit.*, pag. 120.

[60] Hotărârea Curții din 11 decembrie 2019, *TK c./Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, EU:C:2019:1064.

B. Directive ale Uniunii Europene

- ⇨ 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 și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului;
- ⇨ Directiva (UE) 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave;
- ⇨ 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);
- ⇨ Directiva 2000/31/CE a Parlamentului European și a Consiliului din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societății informaționale, în special ale comerțului electronic, pe piața internă (directiva privind comerțul electronic).

C. Decizii ale Uniunii Europene

- ⇨ Decizia Comisiei 2010/87/UE din 5 februarie 2010 privind clauzele contractuale tip pentru transferul de date cu caracter personal către persoanele împuternicite de către operator stabilite în țări terțe în temeiul Directivei 95/46/CE;
- ⇨ Decizia Consiliului 2010/365/UE din 29 iunie 2010 privind aplicarea dispozițiilor acquis-ului Schengen referitoare la Sistemul de Informaţii Schengen în Republica Bulgaria şi în România;
- ⇨ Decizia Consiliului 2009/371/JAI din 6 aprilie 2009 privind înființarea Oficiului European de Poliție (Europol);
- ⇨ Decizia Consiliului 2008/633/JAI din 23 iunie 2008 privind accesul la Sistemul de Informaţii privind vizele (VIS) în vederea consultării de către autoritățile desemnate ale statelor membre şi de către Europol în scopul prevenirii, depistării şi cercetării infracţiunilor de terorism şi a altor infracţiuni grave;
- ⇨ Decizie-cadru 2008/977/JAI privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală;
- ⇨ Decizia Comisiei din 4 martie 2008 de adoptare a Manualului SIRENE şi a altor dispoziţii de aplicare a Sistemului de Informaţii Schengen din a doua generaţie (SIS II);
- ⇨ Decizia 2007/533/JAI din 27 iunie 2007 privind instituirea, funcţionareaşi utilizarea Sistemului de Informaţii Schengen din a doua generaţie;
- ⇨ Decizia Comisiei 2004/915/CE din 27 decembrie 2004 de modificare a Deciziei 2001/497/CE privind introducerea unui set alternativ de clauze contractuale standard pentru transferul de date cu caracter personal către țări terțe;
- ⇨ Decizia Comisiei 2001/497/CE din 15 iunie 2001 privind clauzele contractuale standard pentru transferul de date cu caracter personal către țările terțe în temeiul Directivei 95/46/CE.

D. Legislație internă

- ⇨ Legea nr. 102/2005 privind înființarea, organizarea şifuncţionareaAutorităţiiNaţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările și completările ulterioare, republicată;
- ⇨ Legea nr. 129/2018 pentru modificarea şi completarea Legii nr. 102/2005 privind înființarea, organizarea şifuncţionareaAutorităţiiNaţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum şi pentru abrogarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date;
- ⇨ Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor);
- ⇨ Legea nr. 363/2018 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracţiunilor sau al executării pedepselor, măsurilor educative şi de siguranţă, precum şi privind libera circulaţie a acestor date;
- ⇨ Legea nr. 682/2001 privind ratificarea Convenţiei pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981;
- ⇨ Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şiprotecţiavieţii private în sectorul comunicaţiilor electronice;
- ⇨ Legea nr. 365/2002 privind comerţul electronic;
- ⇨ Norme metodologice din 20 noiembrie 2002 pentru aplicarea Legii nr. 365/2002 privind comertul electronic;
- ⇨ Legea nr. 146/2008 pentru aderarea României la Tratatul dintre Regatul Belgiei, Republica Federală Germania, Regatul Spaniei, Republica Franceză, Marele Ducat de Luxemburg, Regatul Ţărilor de Jos şi Republica Austria privind aprofundarea cooperării transfrontaliere, în special în vederea combaterii terorismului, criminalităţii transfrontaliere şimigraţiei ilegale, semnat la Prum la 27 mai 2005;
- ⇨ Regulamentul de Organizare şi Funcţionare al ANSPDCP din 11 Noiembrie 2005, cu modificările şi completările ulterioare.

E. Decizii ale Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal

- ⇨ Decizia nr. 99/2018 privind încetarea aplicabilităţii unor acte normative cu caracter administrativ emise în aplicarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date;
- ⇨ Decizia nr. 128/2018 privind aprobarea formularului tipizat al notificării de încălcare a securităţii datelor cu caracter personal în conformitate cu Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE;
- ⇨ Decizia nr. 133/2018 privind aprobarea Procedurii de primire și soluționare a plângerilor;
- ⇨ Decizia nr. 161/2018 privind aprobarea Procedurii de efectuare a investigațiilor;

- ⇨ Decizia nr. 238/2019 privind modificarea anexei nr. 2 la Procedura de efectuare a investigațiilor;
- ⇨ Decizia nr. 174/2018 privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor cu caracter personal.

F. Opinii ale Grupului de lucru art. 29

- ⇨ Avizul 2/2014 referitor la un referențial privind cerințele pentru regulile corporatiste obligatorii prezentate autorităților naționale de protecție a datelor din UE și pentru regulile transfrontaliere privind protecția vieții private prezentate agenților APEC cu responsabilități în materie de CBPR, adoptat la 27 februarie 2014;
- ⇨ Avizul 3/2014 privind notificarea încălcărilor securității datelor cu caracter personal, adoptat la 25 martie 2014;
- ⇨ Avizul 4/2014 privind supravegherea comunicațiilor electronice în scopul colectării de date operative și al asigurării securității naționale, adoptat la 10 aprilie 2014;
- ⇨ Avizul 5/2014 privind tehnicile de anonimizare, adoptat la 10 aprilie 2014;
- ⇨ Avizul 6/2014 privind noțiunea de interese legitime ale operatorului de date în conformitate cu articolul 7 din Directiva 95/46/CE, adoptat la 9 aprilie 2014;
- ⇨ Avizul 7/2014 privind protecția datelor cu caracter personal în Quebec, adoptat la 4 iunie 2014.

G. Documente fără forță juridică obligatorie:

- ⇨ Ghiduri emise de Comitetul European pentru Protecția Datelor;
- ⇨ Documente ale Comitetului European pentru Protecția Datelor;
- ⇨ Ghiduri emise de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal;
- ⇨ Alte materiale informative destinate aplicării Regulamentului General privind Protecţia Datelor, emise de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal;
- ⇨ Intrebări frecvente adresate Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal;
- ⇨ Comunicate ale Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal privind participarea la evenimente dedicate Regulamentului General privind Protecţia Datelor.

Aspecte generale privind drepturile și obligațiile instituțiilor și ale persoanelor implicate în prelucrarea datelor cu caracter personal

Prelucrarea datelor cu caracter personal poate fi realizată de către instituții și/sau persoane potrivit Regulamentului (UE) 2016/679. Calitatea pe care urmează să o îndeplinească se stabilește de la început pentru a asigura drepturile și obligațiile în prelucrarea datelor cu caracter personal , chiar dacă aceasta (prelucrare) are loc sau nu pe teritoriul Uniunii.

Astfel, există următoarele categorii de entități, respectiv persoane fizice, implicate în prelucrarea datelor cu caracter personal:

- ⇨ „operator”
- ⇨ „persoană împuternicită de operator”

- ⇨ operatori asociați
- ⇨ terți
- ⇨ „persoana vizată” este persoana ale cărei date cu caracter personal sunt prelucrate.

A. În calitate de *operator,* obligațiile acestuia suntreglementate în Capitolul IV din Regulamentul (UE) 2016/679.

Printre cele mai relevante obligații ale operatorilor în aplicarea Regulamentuluile evidențiem pe următoarele:

- ⇨ respectarea principiilor de prelucrare a datelor (art. 5 din Regulament);
- ⇨ respectarea drepturilor persoanelor fizice (art. 12-23 din Regulament);
- ⇨ asigurarea securității datelor (art. 25 și art. 32 din Regulament);
- ⇨ desemnarea unui responsabil cu protecția datelor (art. 37-39 dinRegulament), după caz;
- ⇨ notificarea încalcărilor de securitate (art. 33 din Regulament), după caz;
- ⇨ evaluarea impactului asupra protecției datelor și respectarea drepturilorpersoanelor fizice (art. 35 din Regulament), după caz;
- ⇨ cartografierea prelucrărilor de date cu caracter personal (art. 30 dinRegulament).

B. Operatorul recurge doar la *persoane împuternicite* care oferă garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte cerințele prevăzute în prezentul regulament și să asigure protecția drepturilor persoanei vizate(art. 28 dinRegulament).

Prelucrarea efectuată de către o persoană împuternicită în numele unuioperator este reglementată printr-un contract sau alt act juridic în temeiuldreptului Uniunii sau al dreptului intern care are caracter obligatoriu pentrupersoana împuternicită de operator în raport cu operatorul şi care stabileşteobiectul şi durata prelucrării, natura şi scopul prelucrării, tipul de date cucaracter personal şi categoriile de persoane vizate şiobligaţiileşi drepturileoperatorului(art. 28 din RGPD).

C. *Operatori asociați* - În cazul în care doi sau mai mulți operatori stabilesc în comun scopurile și mijloacele de prelucrare, aceștia sunt operatori asociați. Ei stabilesc într-un mod transparent responsabilitățile fiecăruia în ceea ce privește îndeplinirea obligațiilor care le revin în temeiul regulamentului, în special în ceea ce privește exercitarea drepturilor persoanelor vizate și îndatoririle fiecăruia de furnizare a informațiilor, prin intermediul unui acord între ei, cu excepția cazului și în măsura în care responsabilitățile operatorilor sunt stabilite în dreptul Uniunii sau în dreptul intern care se aplică acestora. Acordul poate să desemneze un punct de contact pentru persoanele vizate.

D. În ce privește*drepturile* persoanei vizate, sediul principal al materiei îl reprezintăCapitolul III din Regulamentul (UE) 2016/679:

- ⇨ dreptul la informare (art. 13 și art. 14);
- ⇨ dreptul de acces (art. 15);
- ⇨ dreptul la rectificare (art. 16);
- ⇨ dreptul la ștergere („dreptul de a fi uitat” – art. 17);
- ⇨ dreptul la restricționarea prelucrării (art. 18);
- ⇨ dreptul la portabilitatea datelor (art. 20);
- ⇨ dreptul la opoziție (art. 21);
- ⇨ dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrareaautomată (art. 22);

⇨ dreptul de a depune o plângere la o autoritate de supraveghere (art. 77).

Pentru exercitarea drepturilor prevăzute la art. 15 – 22 din Regulamentul(UE) 2016/679, este necesar ca persoanele vizate să adreseze o cerereoperatorului în acest sens(Ghid -Întrebări și răspunsuri cu privire la aplicarea Regulamentului (UE) 2016/679).

În mod corelativ, există astfel de drepturi și obligații atât în privința persoanelor împuternicite de operator (art. 25 ș.a. din RGPD), operatorilor asociați (art. 26 din RGPD) și a terților.

Principii privind prelucrarea datelor cu caracter personal

Sediul materiei: art. 5 RGDP

Principiile privind prelucrarea datelor cu caracter personal sunt:

1. Principiul legalității, echității și transparenței potrivit căruia datele cu caracter personal sunt prelucrate în mod legal, echitabil și transparent față de persoana vizată.

Potrivit art. 6 alin. (1) din Regulament, prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:

- persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;
- prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;
- prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;
- prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;
- prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;
- prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

Temeiul pentru prelucrarea datelor în vederea îndeplinirii unei obligații legale care îi revine operatorului și în cazul în care prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță trebuie să fie prevăzut în dreptul Uniunii sau în dreptul intern care se aplică operatorului.

Scopul prelucrării este stabilit pe baza respectivului temei juridic sau, în ceea ce privește prelucrarea pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul, este necesar pentru îndeplinirea unei sarcini efectuate în interes public sau în cadrul exercitării unei funcții publice atribuite operatorului. Respectivul temei juridic poate conține dispoziții specifice privind adaptarea aplicării normelor prezentului regulament, printre altele:

- condițiile generale care reglementează legalitatea prelucrării de către operator;
- tipurile de date care fac obiectul prelucrării;

- persoanele vizate;
- entitățile cărora le pot fi divulgate datele și scopul pentru care respectivele date cu caracter personal pot fi divulgate;
- limitările legate de scop;
- perioadele de stocare și
- operațiunile și procedurile de prelucrare, inclusiv măsurile de asigurare a unei prelucrări legale și echitabile.

Dreptul Uniunii sau dreptul intern urmărește un obiectiv de interes public și este proporțional cu obiectivul legitim urmărit.

În cazul în care prelucrarea în alt scop decât cel pentru care datele cu caracter personal au fost colectate nu se bazează pe consimțământul persoanei vizate sau pe dreptul Uniunii sau dreptul intern, operatorul, pentru a stabili dacă prelucrarea în alt scop este compatibilă cu scopul pentru care datele cu caracter personal au fost colectate inițial, ia în considerare, printre altele:

- orice legătură dintre scopurile în care datele cu caracter personal au fost colectate și scopurile prelucrării ulterioare preconizate;
- contextul în care datele cu caracter personal au fost colectate, în special în ceea ce privește relația dintre persoanele vizate și operator;
- natura datelor cu caracter personal, în special în cazul prelucrării unor categorii speciale de date cu caracter personal sau în cazul în care sunt prelucrate date cu caracter personal referitoare la condamnări penale și infracțiuni;
- posibilele consecințe asupra persoanelor vizate ale prelucrării ulterioare preconizate;
- existența unor garanții adecvate, care pot include criptarea sau pseudonimizarea.

2. Principiul limitării legate de scopul prelucrării datelor cu caracter personal, potrivit căruia aceste date sunt colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale, în conformitate cu articolul 89 alineatul (1).

3. Principiul reducerii la minimum a datelor prelucrate – în acest sens, datele cu caracter personal trebuie să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate.

Potrivit considerentului 78 din preambulul Regulamentului, protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal necesită adoptarea de măsuri tehnice și organizatorice corespunzătoare pentru a se asigura îndeplinirea cerințelor din prezentul regulament. Pentru a fi în măsură să demonstreze conformitatea cu prezentul regulament, operatorul ar trebui să adopte politici interne și să pună în aplicare măsuri care să respecte în special principiul protecției datelor începând cu momentul conceperii și cel al protecției implicite a datelor. Astfel de măsuri ar putea consta, printre altele, în reducerea la minimum a prelucrării datelor cu caracter personal.

Având în vedere stadiul actual al tehnologiei, costurile implementării, și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, pune în aplicare măsuri tehnice și organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la

minimum a datelor, și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele prezentului regulament și a proteja drepturile persoanelor vizate (art. 25 alin. (1) din RGPD).

4. Principiul exactității – datele cu caracter personal trebuie să fie exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere.

5. Principiul limitării stocării–cu privire la acest principiu, este necesar ca datele cu caracter personal să fie păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor și libertăților persoanei vizate.

6. Principiul integrității și confidențialității vizează faptul că datele cu caracter personal sunt prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare.

7. Principiul responsabilității se referă la faptul că operatorul este responsabil de respectarea tuturor principiilor de mai sus.

Potrivit art. 82 din RGPD, orice persoană care a suferit un prejudiciu material sau moral ca urmare a unei încălcări a regulamentului are dreptul să obțină despăgubiri de la operator sau de la persoana împuternicită de operator pentru prejudiciul suferit.

Orice operator implicat în operațiunile de prelucrare este răspunzător pentru prejudiciul cauzat de operațiunile sale de prelucrare care încalcă regulamentul. Persoana împuternicită de operator este răspunzătoare pentru prejudiciul cauzat de prelucrare numai în cazul în care nu a respectat obligațiile din regulament care revin în mod specific persoanelor împuternicite de operator sau a acționat în afara sau în contradicție cu instrucțiunile legale ale operatorului.

Operatorul sau persoana împuternicită de operator este exonerat(ă) de răspundere dacă dovedește că nu este răspunzător (răspunzătoare) în niciun fel pentru evenimentul care a cauzat prejudiciul.

În cazul în care mai mulți operatori sau mai multe persoane împuternicite de operator, sau un operator și o persoană împuternicită de operator sunt implicați (implicate) în aceeași operațiune de prelucrare și răspund pentru orice prejudiciu cauzat de prelucrare, fiecare operator sau persoană împuternicită de operator este răspunzător (răspunzătoare) pentru întregul prejudiciu pentru a asigura despăgubirea efectivă a persoanei vizate.

Dacă un operator sau o persoană împuternicită de operator a plătit în totalitate despăgubirile pentru prejudiciul ocazionat, respectivul operator sau respectiva persoană împuternicită de operator are dreptul să solicite de la ceilalți operatori sau celelalte persoane împuternicite de operator implicate în aceeași operațiune de prelucrare

recuperarea acelei părți din despăgubiri care corespunde părții lor de răspundere pentru prejudiciu.

Acțiunile în exercitarea dreptului de recuperare a despăgubirilor plătite se introduc la instanțele competente în temeiul dreptului statului membru.

8. Principiul proporționalității - prelucrarea datelor cu caracter personal trebuie să fie în serviciul cetățenilor. Dreptul la protecția datelor cu caracter personal nu este un drept absolut; acesta trebuie luat în considerare în raport cu funcția pe care o îndeplinește în societate și echilibrat cu alte drepturi fundamentale (considerentul 8 din preambulul Regulamentului (UE) 2016/679).

9. Principiul accesului public la documente oficiale – în temeiul acestui principiu, accesul public la documente oficiale poate fi considerat a fi în interes public. Datele cu caracter personal din documentele deținute de o autoritate publică sau de un organism public ar trebui să poată fi divulgate de autoritatea respectivă sau de organismul respectiv în cazul în care dreptul Uniunii sau dreptul intern sub incidența căruia intră autoritatea publică sau organismul public prevede acest lucru. Dreptul Uniunii și dreptul intern ar trebui să asigure un echilibru între accesul public la documentele oficiale și reutilizarea informațiilor din sectorul public, pe de o parte, și dreptul la protecția datelor cu caracter personal, pe de altă parte, și ar putea prin urmare să prevadă echilibrul necesar cu dreptul la protecția datelor cu caracter personal în temeiul prezentului regulament. Trimiterea la autoritățile și organismele publice ar trebui, în acest context, să includă toate autoritățile sau alte organisme reglementate de dreptul intern privind accesul public la documente (considerentul 154 din preambulul Regulamentului (UE) 2016/679).

CAP II. IDENTIFICAREA MODALITĂȚILOR ȘI INSTRUMENTELOR DE MONITORIZARE A MODULUI ÎN CARE INSTITUȚIA /AUTORITATEA RESPECTA PREVEDERILE ÎN DOMENIUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL, ORGANIZAREA ȘI UTILIZAREA ACESTORA ÎN CADRUL INSTITUȚIEI/AUTORITĂȚII.

Instrumente de monitorizare a activităților de prelucrare de date cu caracter personal:

- Desemnarea unui responsabil cu protecția datelor cu caracter personal DPO
- Cartografierea registrului activităţilor de prelucrare
- Managementul politicilor și procedurilor organizatiei
- Stabilirea unor responsabili pe activităţi şi procese
- Analiza detaliată a activităţilor şi alocarea resurselor necesare
- Formarea continuă a angajaţilor care operează DCCP
- Externalizarea unor servicii cu riscuri mari şi stabilirea modului de lucru
- Analiza detaliată în prelucrarea DCCP împreună cu alţi operatori
- Auditarea şi reactualizarea periodică a activităților cu risc mare
- Managementul riscurilor

Operatorul și persoana împuternicită de operator desemnează un responsabil cu protecția datelor ori de câte ori:

- activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrare care, prin natura, domeniul de aplicare și/sau scopurile lor, necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă;
- sau activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date, menționată la articolul 9, și art 10.

Desemnarea unui Responsabil cu protecţia datelor cu caracter personal este obligatorie când se impune monitorizarea periodică a activităţilor de prelucrare.

Pentru a putea monitoriza modul în care instituția respectă prevederile în domeniul prelucrării datelor cu caracter personal, trebuie stabilite modalitățiile și instrumentele de monitorizare în funcție de fluxurile de prelucrare date la instituția/operatorul de date și de gradul de risc aferent.

1. Identificarea și gestionarea riscurilor

1.1.Cartografierea fluxurilor de prelucrare

Cartografierea datelor este un sistem de catalogare a datelor pe care le colectați, modul în care sunt utilizate, unde sunt stocate și fluxul acestora în întreaga organizație și în afara acesteia.

Există mai multe modalități de a atinge acest obiectiv – fie printr-o foaie de calcul simplă, fie printr-un program dedicat cartografierii datelor.

Cartografierea este un registru în care se regăsesc toate activităţile importante prin care se prelucrează date cu caracter personal şi care pot genera riscuri pentru persoana vizată. Respectiva evidență cuprinde toate următoarele informații:

(a) numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;

(b) scopurile prelucrării;

(c) o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal; 4.5.2016 L 119/50 Jurnalul Oficial al Uniunii Europene RO

(f) acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;

(g) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 32 alineatul (1).

Fiecare operator și, după caz, persoana împuternicită de operator păstrează o evidență a tuturor categoriilor de activități de prelucrare desfășurate în numele operatorului, care cuprind:

(a) numele și datele de contact ale persoanei sau persoanelor împuternicite de operator și ale fiecărui operator în numele căruia acționează această persoană (aceste persoane), precum și ale reprezentantului operatorului sau al persoanei împuternicite de operator, după caz;

(b) categoriile de activități de prelucrare desfășurate în numele fiecărui operator;

Cartografierea eficientă de date necesită monitorizarea îndeaproape a fiecărui departament, în special a departamentelor :

- IT,
- Juridic,
- Marketing și Resurse Umane.

În plus, documentarea tuturor datelor trebuie atent supravegheată de către **Responsabilul cu protecția datelor(DPO)** sau de un membru al echipei de management.

1.2.Activități premergătoare cartografierii:

- ***Inventarierea datelor***: - Care sunt datele cu caracter personal prelucrate?
- ***Stabilirea unei baze legale*** - În ce temei sunt prelucrate datele cu caracter personal?
- Transparența informațiilor:
    - Unde sunt stocate datele colectate?
    - Cine are autorizarea de a prelucra datele (vizualizare/modificare/ștergere)?
- ***Stabilirea fluxului de date: -*** Sistemele organizației tale transferă automat informații către alte sisteme informatice?

1.3. Pași pentru realizarea cartografierii

- ***Analiza documentației interne:*** - Analiza ROI, ROF și Organigramă în vederea planificării cartografierii
- ***Planificarea cartografierii:*** - Identificarea departamentelor/ serviciilor/birourilor din cadrul Organizației, selectarea personalului pe care îl vom implica în proiect și transmiterea instrumentelor de lucru.
- ***Instruirea: -*** Din experiența acumulată, 75% din personal nu înțelege necesitatea cartografierii, este refractară la această idee și de aceea nu înțelege în mod direct cum se completează un tabel de cartografiere, 15% înțeleg dar nu în totalitate, și 10% înțeleg și realizează completarea tabelului în mod corect, în termen și fără erori mari.
- ***Oferirea de asistență personală:*** - Este utilă oferirea de sprijin personalului departamentelor în vederea completării tabelelor (o întâlnire minim / departament)
- ***Colectarea tabelelor de cartografiere:*** - Această etapă poate dura de la 1 la 8 săptămâni

Analiza tabelelor și rectificarea după caz a formei inițiale:

- Care prelucrări de date sunt obligatorii prin lege și care nu sunt, unde este vorba despre o informare a persoanelor vizate și unde este vorba despre necesitatea unui consimțământ?
- Cine are acces la aceste date?
- Unde se face transfer de date, modalitatea și riscurile pe care un astfel de transfer le implică?
- Posibile prelucrări de date neintenționate sau despre care nu se știa

- Stabilirea perioadei de retenție – obligație legală/ termen rezonabil – se recomandă consultarea nomenclatorul arhivistic și legislația națională.
- Necesitatea distrugerii securizate a documentelor: implementarea unor proceduri /achiziționarea unui tocător de hârtie / furnizor extern de servicii.

- ***Finalizarea tabelului de cartografiere și realizarea diagramelor: -*** Tabelul va ilustra fluxul de date, în baza tuturor mini-tabelelor completate

- ***Trimitere formă inițială spre analiză:***
- ***Finalizarea diagramelor, printarea și distribuirea și afișarea acestora:*** - afișarea proceselor de prelucrare a datelor cu caracter personal este una dintre cele mai eficiente modalități de informare a persoanelor vizate. Mai mult decât atât, afișarea proceselor de prelucrare este în conformitate cu principiul transparenței şi duce la creșterea nivelului de încredere în organizație.
- ***Realizarea politicii de prelucrare a datelor: -*** Procesul de cartografiere va sta la baza întocmirii Politicii de prelucrare a datelor

Problemele pe care le putem întâlni în realizarea cartografierii

Cartografierea este percepută ca fiind:

1. Prea costisitoare de timp pentru a fi realizată
2. Neînțeleasă
3. Neprioritară
4. Contradictorie
5. Un proiect ce trebuie bifat.

Ce facem?

1. Sistematizăm informațiile
2. Avem instruiri și vizite personale la fiecare departament
3. Găsim persoana potrivită care să ne ofere sprijin
4. Facem o dublă verificare
5. Adaptăm produsul.

2. Codul de conduită

Codul de conduită prevăzut la alineatul (2) din prezentul articol cuprinde mecanisme care permit organismului menționat la articolul 41 alineatul (1) să efectueze monitorizarea obligatorie a respectării dispozițiilor acestuia de către operatorii sau persoanele împuternicite de operatori care se angajează să îl aplice, fără a aduce atingere sarcinilor și competențelor autorităților de supraveghere care sunt competente în temeiul articolului 55 sau 56.

Fără a aduce atingere sarcinilor și competențelor autorității de supraveghere competente în temeiul articolelor 57 și 58, monitorizarea respectării unui cod de conduită în temeiul articolului 40 poate fi realizată de un organism care dispune de un nivel adecvat de expertiză în legătură cu obiectul codului și care este acreditat în acest scop de autoritatea de supraveghere competentă.

(2)Un organism menționat la alineatul (1) poate fi acreditat pentru monitorizarea respectării unui cod de conduită dacă:

(a) a demonstrat autorității de supraveghere competente, într-un mod satisfăcător, independența și expertiza sa în legătură cu obiectul codului;

Respectiva evidență cuprinde toate următoarele informații:

(a) numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;

(b) scopurile prelucrării;

(c) o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal; 4.5.2016 L 119/50 Jurnalul Oficial al Uniunii Europene RO

(f) acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;

(g) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 32 alineatul (1).

Fiecare operator și, după caz, persoana împuternicită de operator păstrează o evidență a tuturor categoriilor de activități de prelucrare desfășurate în numele operatorului, care cuprind:

(a) numele și datele de contact ale persoanei sau persoanelor împuternicite de operator și ale fiecărui operator în numele căruia acționează această persoană (aceste persoane), precum și ale reprezentantului operatorului sau al persoanei împuternicite de operator, după caz;

(b) categoriile de activități de prelucrare desfășurate în numele fiecărui operator;

Operatorul păstrează o evidență a tuturor categoriilor de activități de prelucrare desfășurate în numele operatorului, care cuprind:

(c) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, în cazul transferurilor prevăzute la articolul 49 alineatul (1) al doilea paragraf, documentația care dovedește existența unor garanții adecvate;

(d) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 32 alineatul (1).

3)Evidențele menționate la alineatele (1) și (2) se formulează în scris, **inclusiv în format electronic**.

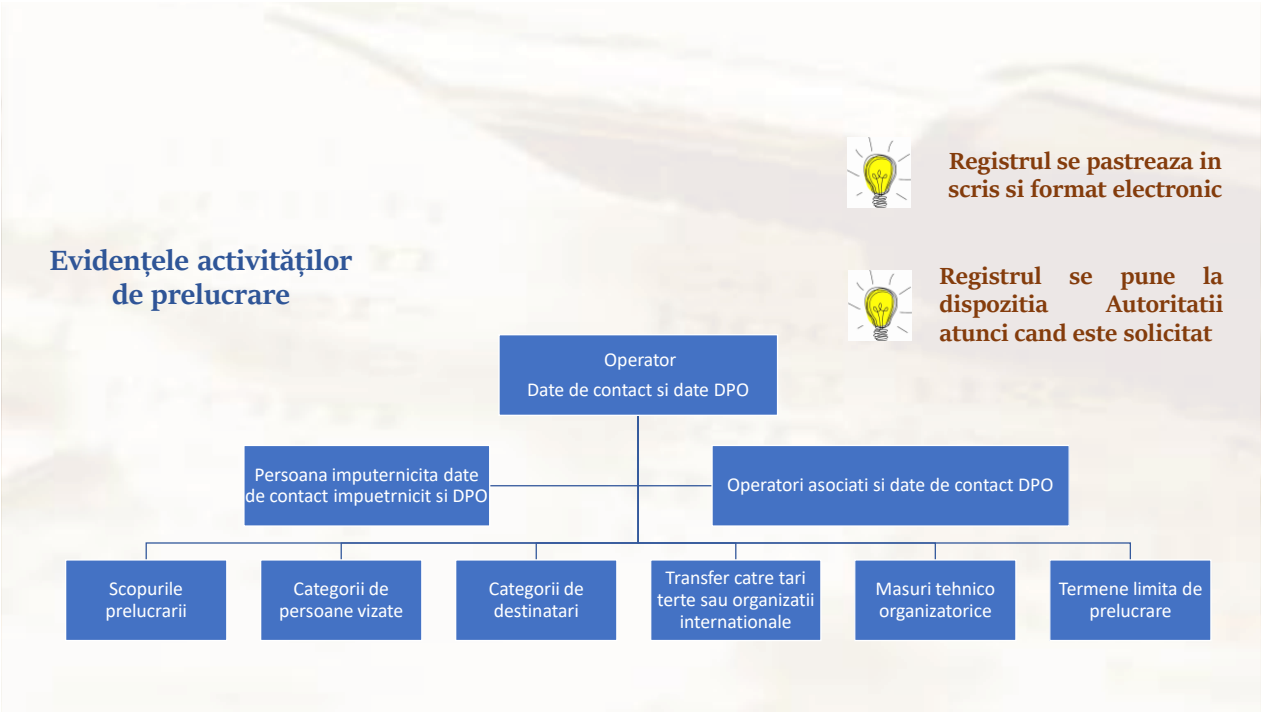
(4)Operatorul sau persoana împuternicită de acesta, precum și, după caz, reprezentantul operatorului sau al persoanei împuternicite de **operator pun evidențele la dispoziția autorității de supraveghere**, la cererea acesteia.

Obligațiile menționate la alineatele 1 și 2 nu se aplică unei întreprinderi sau organizații cu mai puțin de **250 de angajați**, cu excepția cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date, astfel cum se prevede la articolul 9 alineatul (1), si articolul 10.

Evidențele activităților de prelucrare

Ce informaţii apar în registru:

- Numele şi datele de contact ale operatorului şi, după caz, ale operatorului asociat, împuternicit, şi DPO-ul fiecăruia.
- Scopurile prelucrării.
- Descrierea categoriilor de persoane vizate.
- Descrierea categoriilor de date cu caracter personal prelucrate în mod constant.
- Descrierea categoriilor de date cu caracter personal prelucrate ocazional.
- Volumul de date cu caracter personal prelucrate.
- Categoriile de destinatari (colaboratori, parteneri) cărora le-au fost sau le vor transmite date cu caracter personal, inclusiv destinatarii din ţări terţe sau organizaţii internaţionale.
- Acolo unde este posibil, termenele-limită preconizate pentru ştergerea diferitelor categorii de date.
- Acolo unde este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate.



Pentru situaţia când monitorizarea este dificilă pentru anumite activităţi şi costurile sunt ridicate, organizaţia poate externaliza anumite servicii.

Atunci când este un efort suficient de mare pentru organizaţie.

Ce avantaje avem?

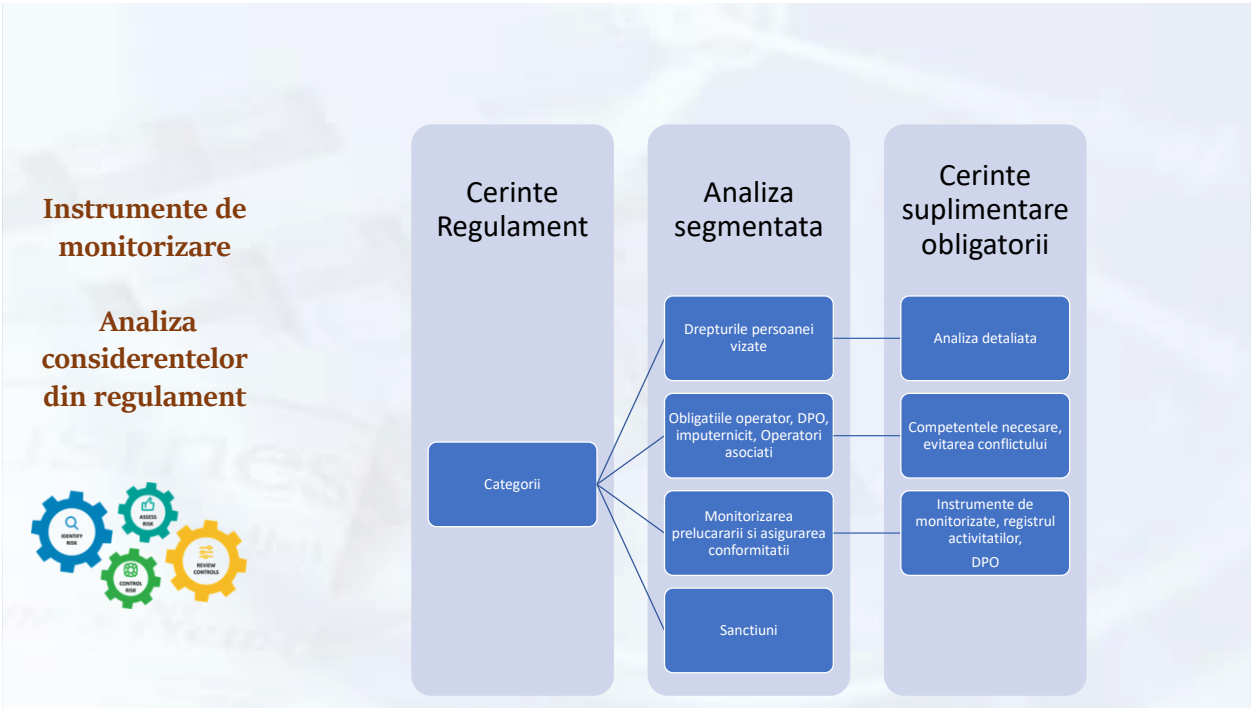
- Eliminarea riscului conflictului de interese
- Externalizarea riscului către o altă organizaţie specializată

• La stabilirea unei persoane din organizaţie, există cheltuieli care se pot transfera către externalizarea acestui serviciu

• Transparenţa - Monitorizare şi auditare externă

• Experienţa şi calificarea personalului desemnat

• Alinierea perfectă la cerinţele Regulamentului UE 679/2016



Politici și instrumente care pot fi aplicate

Politici și instrumente care pot fi aplicate în vederea monitorizării modului în care organizația respectă prevederile legislației privind protecția datelor cu caracter personal.

Un instrument folosit pentru monitorizarea activităţilor de prelucrări de date cu caracater personal este elaborarea de politici şi proceduri de către organizaţie.

Politicile sunt principii de ordin general aplicabile pentru domenii. De exemplu politica securităţii informaţionale.

Procedurile sunt instrumente care stabilesc modul de prelucrare a unei activităţi detaliate.

Procedura documentată – Descrierea unei activităţi sau a unui proces, editat pe suport hârtie sau în format electronic; procedurile documentate pot fi proceduri de sistem şi proceduri operaţionale.

Procedura operațională (procedura de lucru) – procedura care descrie un proces sau o activitate care se desfăşoară la nivelul unuia sau mai multor compartimente dintr-o entitate, fără aplicabilitate la nivelul întregii entităţi publice.

Procedura de sistem (procedura generală) – descrie un proces sau o activitate care se desfașoară la nivelul entității publice aplicabil/aplicabilă majorității sau tuturor compartimentelor dintr-o entitate publică.

Activitate procedurală - proces major sau activitate pentru care se pot stabili modalităţi de lucru, general valabile, în vederea îndeplinirii, în condiţii de legalitate, eficienţă, eficacitate, aplicabile unui compartiment și/sau organizatiei.

Actualizare procedură – constă fie în revizuirea procedurii fie în elaborarea unei noi ediții a acesteia.

Cartuș procedură – text încadrat în chenar, pe o pagină imprimată.

Compartiment - direcție generală, direcție, departament, serviciu, birou, comisie, inclusiv instituție/structură fără personalitate juridică aflată în subordinea, coordonarea sau sub autoritatea entității.

Orice modificare a procedurii va fi făcuta sub forma unei revizii.

Ediție procedură - forma actuală a procedurii; ediția unei proceduri se modifică atunci când deja au fost realizate de regulă trei revizii ale respectivei proceduri sau atunci când modificările din structura procedurii depășesc 50% din conținutul reviziei anterioare.

Dupa fiecare modificare, procedura va fi supusă aprobării conducerii și va fi *difuzată personalului implicat*

Procedurile pe care o entitate le aplică pentru tratarea riscului sunt denumite activități de control intern.

Activitățile de control intern sunt un raspuns la risc în sensul că sunt proiectate să conțină nesiguranța rezultatelor ce au fost identificate.

Activitate procedurală – proces major sau activitate semnificativă pentru care se pot stabili reguli și modalități de lucru, general valabile, în vederea îndeplinirii, în condiții de regularitate, eficacitate, economicitate și eficiență a obiectivelor compartimentului și/sau entității publice.

Componente importante din cadrul unei proceduri:

- Stabilirea unui responsabil de proces.
- Stabilirea bazei legale la care se supune activitatea.
- Descrierea detaliată a activității.
- Modul prin care se difuzeaza procedura către personalul operator.
- Resursele puse la dispoziție

Cuprinsul unei proceduri

- Lista responsabililor cu elaborarea, verificarea, aprobarea ediţiei şi a reviziei în cadrul ediţiei
- Formular de evidență a modificărilor
- Formularul de distribuire/difuzare
- Definitii și abrevieri
- Scopul procedurii
- Domeniul de aplicare
- Baza legislativă
- Descrierere activității sau a procesului
- Documente utilizate
- Resurse necesare
- Anexe și diagrame de flux

Lista nu este exaustivă, poate să aibe un conținut diferit dar trebuie să stabilească modul de operare, resurse, actorii cheie, responsabili și personal operator.

Cartușul procedurii

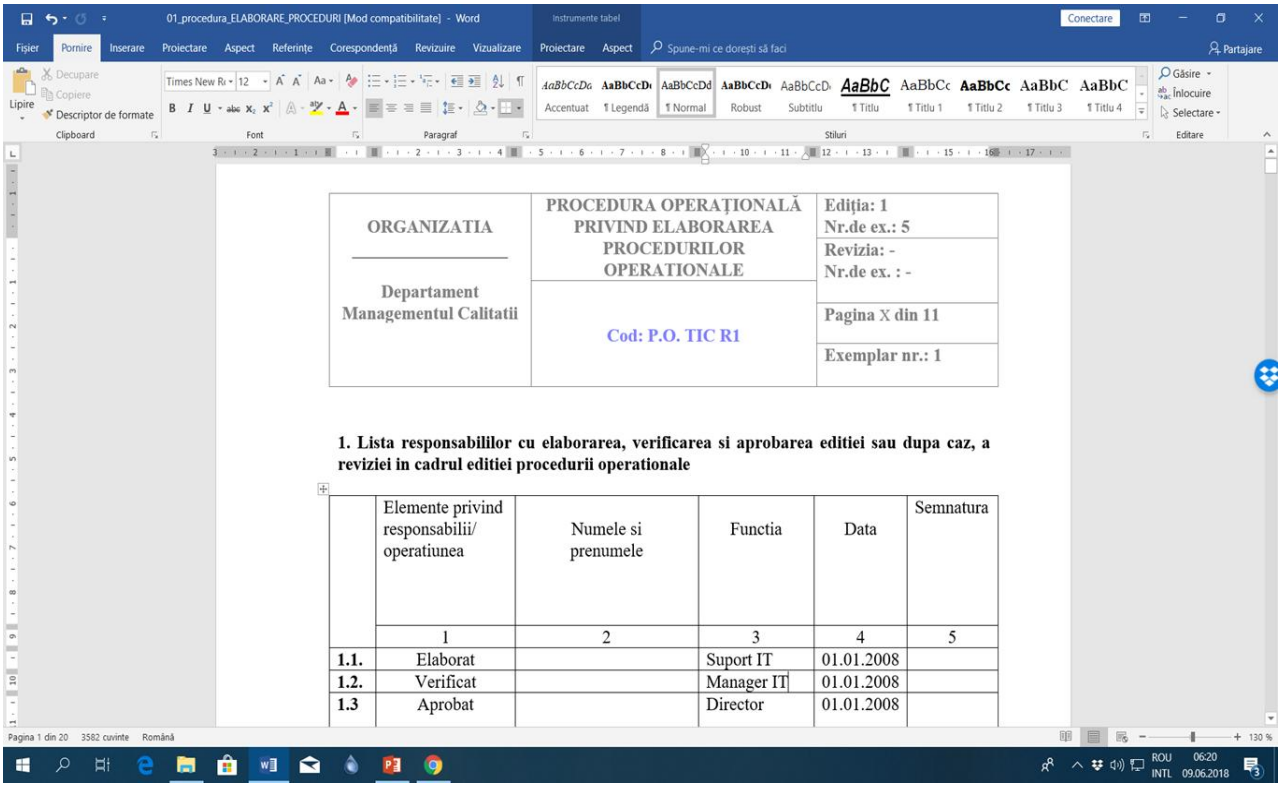
Datele de identificare privind denumirea entității publice, tipul procedurii, denumirea, codul, numărul de ordine al ediției și reviziei în vigoare, numărul de ordine al exemplarului difuzat unui anumit compartiment, sunt cuprinse într-un format tabelar, denumit cartușul procedurii, conform modelului orientativ de mai jos.

Codificarea procedurii este alocarea unui cod alocat în funcție de denumirea procedurii și compartimentul în care loc activitatea.

Numele procedurii – simbolizează activitatea la care face referire pentru identificare ușoară.

Revizia și ediția din cartuș se modifică corespunzator la fiecare actualizare.

Cum arată cartușul unei proceduri



ORGANIZATIA Departament Managementul Calitatii	PROCEDURA OPERAȚIONALĂ PRIVIND ELABORAREA PROCEDURILOR OPERATIONALE Cod: P.O. TIC R1	Ediția: 1 Nr.de ex.: 5 Revizia: - Nr.de ex. : - Pagina X din 11 Exemplar nr.: 1

1. Lista responsabililor cu elaborarea, verificarea si aprobarea editiei sau dupa caz, a reviziei in cadrul editiei procedurii operationale

	Elemente privind responsabilii/ operatiunea	Numele si prenumele	Functia	Data	Semnatura
	1	2	3	4	5
1.1.	Elaborat		Suport IT	01.01.2008	
1.2.	Verificat		Manager IT	01.01.2008	
1.3	Aprobat		Director	01.01.2008	

Cuprinsul unei proceduri

Sistemul de codificare al procedurilor

Codul procedurii de sistem are în componenţa PS urmat de mai multe cifre sau litere

Ex: PS – xxx

Codul procedurii operaţionale este de tipul PO – XX-YY

Se va specifica şi codul departamentului activităţii procedurale

Ex PO-RUNOS-AS1

Scopul procedurii

Scopul unei proceduri documentate este de a descrie într-un mod structurat o activitate sau proces.

Procedura care descrie o activitate aferentă unui departament sau mai multe, va fi o procedură operațională.

Procesele sau activitățile care se desfasoară în întreaga organizație vor fi intr-o procedură de sistem.

Descrierea procedurii

Descrierea procedurii relatează cum trebuie desfăşurată activitatea sau procesul în succesiune logică, indicarea actorilor implicați în procedură, responsabili de proces etc.

Este cel mai important capitol al procedurii, indicând desfăşurarea fluxului, rolul fiecărui operator în activitate.

Descrierea trebuie să conţină şi circuitul documentelor din cadrul activității dar și formularele folosite în această activitate.

Etapele de realizare a unei proceduri

- Etapa I stabilirea activităților procedurale de sistem și a responsabililor cu elaborarea procedurii;
- Este identic elaborarii Registrului activităţilor de prelucrare a datelor cu caracter personal, sau Registrul riscurilor;
- Etapa II elaborarea propriu-zisă a procedurii;
- Etapa III verificarea, avizarea și aprobarea procedurii;
- Etapa IV distribuirea (difuzarea) procedurii;
- Etapa V actualizarea și arhivarea.

Responsabilul cu elaborarea și actualizarea procedurii

- elaborează evidența activităților procedurale pentru procedurile operaționale de la nivelul compartimentului;
- elaborează Diagrama de proces a procedurii;
- elaborează procedura operațională;
- efectuează modificări și completări ale procedurii;
- înregistrează procedura operațională;
- Dupa aprobarea procedurii, distribuie copii ale procedurii aprobate conform Formularului de distribuire/difuzare;
- îndosariază originalele procedurilor aprobate;
- actualizează procedura operațională;
- arhivează procedurile operaționale retrase;

Evidența modificărilor aduse unei proceduri

- Se întocmește o fișa pentru fiecare procedura în parte în care sunt notate individual fiecare modificare a procedurii.
- Ce conține fișa modificărilor aduse?
  - Ediția si data ediției
  - Revizia și data reviziei
  - Numărul paginei modificate
  - Modificarea efectuată
  - Cine a aprobat modificarea

Actualizarea procedurilor documentate implică una din formele

Revizuirea procedurii, constă în:

- Orice modificare din activitatea sau procesul aferent procedurii necesită o actualizare;
- Schimbarea responsabilului;
- Detalierea unor activități care nu au fost suficient de bine prezentate anterior;
- Modificări prin care și alte compartimente interfereaza cu activitatea procedurală.

4.Politica de confidențialitate

Politica de confidențialitate a unui operator de date trebuie să aibă următorul cuprins minim conform modelul prezentat mai jos:

POLITICĂ DE CONFIDENȚIALITATE

CU PRIVIRE LA PROTECȚIA DATELOR CU CARACTER PERSONAL

Din **25 mai 2018** devine aplicabil **Regulamentul European 2016/679** privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date.

Scopul principal al acestuia este creșterea nivelului de protecție a datelor personale și crearea unui climat de încredere care să permită fiecărei persoane controlul asupra propriilor date.

Conform prevederilor regulamentului, dorim să te **INFORMĂM** cum protejăm datele tale personale și cum ne conformăm prevederilor acestuia.

Ce date personale prelucrăm?

Datele personale pe care le prelucrăm sunt, în principal, datele tale de identificare, demografice, de localizare sau alte date personale pe care le colectăm direct de la tine atunci când devii clientul nostru, sau când folosești produsele sau serviciile noastre.

Cum prelucrăm datele tale personale?

Prelucrăm datele personale doar pentru scopuri legitime, precum acela de a-ți furniza produse și servicii specifice firmei noastre, pentru îmbunătățirea și dezvoltarea produselor și serviciilor pe care ți le oferim. Prelucrarea datelor personale se întemeiază întotdeauna fie pe executarea contractelor încheiate cu noi, pe nevoia de a respecta o obligație legală, pe interesul nostru legitim sau un interes public major sau, după caz, pe consimțământul tău dacă ți-ai manifestat opțiunea în acest sens.

Comunicăm datele tale personale către alți destinatari?

Pentru a-ți oferi servicii cât mai competitive, pentru a executa tranzacțiile pe care le inițiezi, pentru îndeplinirea obligatiilor legale ce ne revin sau în alte scopuri

legitime este posibil să transmitem datele tale personale către autorități publice, organe judiciare, birouri notariale, asigurându-ne însă întotdeauna că instituim garanții adecvate pentru protejarea datelor tale.

Cât timp prelucrăm datele tale personale?

Datele tale personale sunt prelucrate până ce ai calitatea de CLIENT al nostru, pe tot parcursul relației noastre contractuale și, după finalizarea acesteia, cel puțin pe perioada impusă de prevederile legale aplicabile în domeniu, inclusiv, dar fără limitare, la dispozițiile privind arhivarea.

Care sunt drepturile tale și cum pot fi exersate?

- **Dreptul la informare** – poți solicita informații privind activitatile de prelucrare a datelor tale personale;
- **Dreptul la rectificare** – poți rectifica datele personale inexacte sau le poți completa;
- **Dreptul la stergerea datelor** ("dreptul de a fi uitat") – poți obține stergerea datelor, în cazul în care prelucrarea acestora nu a fost legală sau în alte cazuri prevăzute de lege;
- **Dreptul la restricționarea prelucrării** – poți solicita restricționarea prelucrării în cazul în care contești exactitatea datelor, precum și în alte cazuri prevazute de lege;
- **Dreptul de opoziție** – poți să te opui, în special, prelucrărilor de date care se întemeiază pe interesul nostru legitim;
- **Dreptul la portabilitatea datelor** - poți primi, în anumite condiții, datele personale pe care ni le-ai furnizat, într-un format care poate fi citit automat sau poți solicita ca respectivele date să fie transmise altui operator;
- **Dreptul de a depune plângere** - poți depune plângere fața de modalitatea de prelucrare a datelor personale la Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal;
- **Dreptul de retragere a consimțământului** – în cazurile în care prelucrarea se întemeiază pe consimțământul tău, ți-l poți retrage oricând. Retragerea consimțământului va avea efecte doar pentru viitor, prelucrarea efectuată anterior retragerii ramânând în continuare valabilă;
- **Drepturi suplimentare** aferente deciziilor automate: poți cere și obține intervenția umană cu privire la respectiva prelucrare, iți poți exprima propriul punct de vedere cu privire la aceasta și poți contesta decizia.

CAP III. *SFERA ACTIVITĂȚILOR AFERENTE ASISTENȚEI DE SPECIALITATE ACORDATE DE RESPONSABILUL PENTRU PROTECȚIA DATELOR CU CARACTER PERSONAL, ELABORAREA PLANULUI DE LUCRU AL ACESTUIA ȘI PROCEDURI DE LUCRU EFICIENTE CARE SĂ SPRIJINE DPO ÎN EXERCITAREA ATRIBUȚIILOR*

Operatorul şi persoana împuternicită de operator desemnează un responsabil cu protecţia datelor ori de câte ori:

a)prelucrarea este efectuată de o autoritate sau un organism public, cu excepţia instanţelor care acţionează în exerciţiul funcţiei lor jurisdicţionale;

b)activităţile principale ale operatorului sau ale persoanei împuternicite de operator constau în operaţiuni de prelucrare care, prin natura, domeniul de aplicare şi/sau scopurile lor, necesită o monitorizare periodică şi sistematică a persoanelor vizate pe scară largă;

c)activităţile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date sau a unor date cu caracter personal referitoare la condamnări penale şiinfracţiuni.

Regulamentul general privind protecția datelor (**"Regulamentul"**) acordă o importanță sporită funcției responsabilului cu protecția datelor, rolul său fiind de a verifica respectarea prevederilor legale specifice, dar și de a contribui la crearea unei culturi a protecției datelor în cadrul organizației.[61]

Astfel, cea mai importantă sarcină a responsabilului cu protecția datelor constă în **acordarea de consultanță în materia protecției datelor cu caracter personal** organizației care l-a numit.

Pentru a duce la îndeplinire această sarcină, responsabilul cu protecția datelor trebuie implicat în elaborarea și implementarea politicilor, procedurilor, documentelor și chiar a măsurilor cu impact asupra datelor cu caracter personal. Responsabilul cu protecția datelor va acorda asistență organizației în orice chestiuni legate de prelucrarea de date cu caracter personal, recomandările sale urmând a fi prezentate organelor de conducere.

Mergând mai departe, activitatea de consultanță presupune și instruirea constantă a managementului, dar mai ales a angajaților, în scopul creșterii gradului de conștientizare a importanței datelor cu caracter personal. Doar în acest fel se poate crea, la nivelul organizației, o cultură a datelor cu caracter personal, scopul urmărit fiind responsabilizarea angajaților care folosesc date cu caracter personal în îndeplinirea atribuțiilor de serviciu.[62]

Frecvența sesiunilor de pregătire organizate de responsabilul cu protecția datelor, cu propriile resurse sau prin furnizori externi specializați, depinde de domeniul de activitate al organizației (în domeniul bancar sau cel al vânzărilor, de exemplu, apreciem că sunt necesare cel puțin sesiuni bianuale de pregătire) și degradul de fluctuație al personalului (recomandabil este ca toți noii angajați să fie instruiți în materia protecției datelor cu caracter personal imediat după angajare).

---

[61]BALBONI, Paolo; COOPER, Daniel; IMPERIALI, Rosalio; MACENAITE, Milda, Legitimate Interest of the Data Controller. New Data Protection Paradigm: Legitimacy Grounded on Appropriate Protection, în International Data Privacy 20 Law, publicat online la data de 02.08.2013, p. 1-8, disponibil la http://idpl.oxfordjournals.org/content/early/2013/08/01/idpl.ipt019.abstract

[62]Hotărârea din 9 noiembrie 2017, Tünkers France/Expert France, Cauza C-641/16, EU:C:2017:847, în special pct. 18, 19 și 20, www.curia.eu

Îndeplinirea acestei sarcini include, de asemenea:

- acordarea de consultanță cu ocazia realizării de analize a impactului operațiunilor de prelucrare asupra datelor cu caracter personal;
- emiterea de recomandări și oferirea de asistență cu privire la interpretarea și aplicarea prevederilor legislației incidente;
- emiterea de recomandări în privința aderării la anumite coduri de conduită sau mecanisme de certificare.

Activitatea de consultanță în materia protecției datelor cu caracter personal nu atrage răspunderea directă a responsabilului cu protecția datelor.

Potrivit Regulamentului, responsabilitatea respectării prevederilor legale aplicabile aparține organizației, în calitate de operator sau persoană împuternicită de operator, aceasta fiind obligată să pună *"în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prevederile Regulamentului"*.

Cu toate acestea, responsabilul cu protecția datelor poate fi ținut responsabil de prejudiciile cauzate organizației care l-a numit în cazul în care recomandările sale sunt vădit lipsite de profesionalism sau sunt neglijente.[63]

O altă sarcină importantă ce trebuie îndeplinită de responsabilul cu protecția datelor este legată de **monitorizarea respectării legislației privind protecția datelor cu caracter personal** de către organizația care l-a numit.

Și de această dată este vorba de o activitate permanentă ce necesită implicarea responsabilului cu protecția datelor, dar și a altor angajați instruiți să asigure respectarea prevederilor legale în activitățile obișnuite de prelucrare.

Responsabilul cu protecția datelor trebuie așadar să verifice și să analizeze constant modul în care datele cu caracter personal sunt prelucrate în cadrul organizației. În acest scop, va realiza audituri stabilite conform unui plan anual de control, va conduce verificări spontane sau tematice, organizația având obligația de a-i asigura accesul neîngrădit la toate datele, persoanele și informațiile de care are nevoie pentru a duce la îndeplinire această sarcina.

Trebuie subliniat faptul că, în organizațiile mari, activitatea de monitorizare este greu de realizat de o singura persoană, astfel încât o posibilă soluție este crearea unei structuri de monitorizare cu implicarea de persoane din toate departamentele specializate.

Această sarcina ar putea fi îndeplinită și prin[64]:

- monitorizarea respectării codurilor de conduită și a standardelor specifice aplicabile domeniului de activitate al organizației în cadrul cărei își desfășoară activitatea;
- supravegherea procesului de cartografiere a proceselor de prelucrare a datelor cu caracter personal și a evidențelor de prelucrare astfel întocmite;
- verificarea modului în care angajații utilizează, în activitatea obișnuită, instrumentele, documentele și procedurile incidente în materia protecției datelor.

[63]Concluziile avocatului general prezentate la 1 februarie 2018, Tietosuojavaltuutettu/Jehovantodistajat – uskonnollinenyhdyskunta, Cauza C-25/17, EU:C:2018:57, în special pct. 39 și 42.

[64]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 privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:02016R0679-20160504

Sarcinile responsabilului cu protecția datelor includ și **monitorizarea eficacității sistemului de management al securității datelor** implementat în cadrul organizației. Așadar, pe lângă componenta juridică, activitatea responsabilului cu protecția datelor trebuie să urmărească și aspectele tehnice ce însoțesc, în mod inevitabil, prelucrările de date cu caracter personal.

Pentru a duce la îndeplinire această activitate, responsabilul cu protecția datelor ar trebui să realizeze evaluări periodice ale sistemelor informatice, să realizeze teste de penetrare (*de regula cu ajutorul unor furnizori specializați de astfel de servicii*) și să propună măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel corespunzător de securitate a operațiunilor de prelucrare a datelor cu caracter personal.[65]

Potrivit Regulamentului, responsabilul cu protecția datelor trebuie să **asigure cooperarea cu autoritatea de supraveghere și cu celelalte autorități publice,** acționând ca punct unic de contact și colaborare în materia protecției datelor cu caracter personal.

În acest scop, responsabilul cu protecția datelor trebuie să formuleze răspunsuri prompte oricăror solicitări legitime ale autorității de supraveghere sau ale altei autorități publice (instanțe judecătorești, parchete, etc.) în ceea ce privește prelucrarea datelor cu caracter personal. Rolul acestuia este de a asigura comunicarea cu aceste autorități și a acționa ca și unic interlocutor din partea organizației care l-a numit.

Cooperarea cu autoritatea competentă de supraveghere (în domeniul protecției datelor), include, de asemenea:

- solicitarea aprobării cu privire la efectuarea anumitor operațiuni de prelucrare;
- consultarea prealabilă în vederea luării unor măsuri adecvate, atunci când evaluarea impactului asupra protecției datelor indică un risc ridicat.

O altă îndatorire a responsabilului cu protecția datelor vizează **asigurarea comunicării cu persoanele vizate**. Așadar, acesta trebuie să acționeze ca și punct de contact pentru toate persoanele vizate ale căror date cu caracter personal sunt prelucrate de organizația care l-a numit.

Prin urmare, una dintre îndatoririle esențiale ale responsabilului cu protecția datelor este legată de analizarea și formularea de răspunsuri solicitărilor persoanelor vizate. În acest scop, orice astfel de solicitare primită de un reprezentant al organizației ar trebui redirecționată imediat responsabilului cu protecția datelor, acesta fiind cel care urmează a efectua cercetările și/sau solicitările interne necesare formulării unui răspuns, în condițiile Regulamentului. Tot acesta va formula răspunsul adresat persoanei vizate.[66]

Acestea sunt, pe scurt, principalele sarcini pe care responsabilul cu protecția datelor trebuie să le îndeplinească în cadrul organizației care l-a numit. Pe lângă cele detaliate anterior, Regulamentul cuprinde însă și o serie de obligații ale operatorilor sau persoanelor împuternicite de operator ce pot fi legate de îndatoriri suplimentare ale responsabilului cu protecția datelor.

Astfel, potrivit Regulamentului, în anumite condiții, operatorul este obligat să păstreze *"o evidență a activităților de prelucrare"*, iar persoana împuternicită de

[65]JOUE, C202/389 7.6.2016 https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex:12016P/TXT
[66]Henri Oberdorff, Nouveaux outils, nouveaux acteur: vers une cybercitoyenneté ?, în volumul "Le monde quivient. Entrepérils et promesses. 2000-2015: un état des droits", coordonatori G. Aschieri, J.-P. Dubois, E. Tartakowsky, P. Tartakowsky, Éditions La Découverte, Paris, 2016, p. 327.

operator este obligată să păstreze *"o evidență a tuturor categoriilor de activități de prelucrare desfășurate în numele operatorului*".[67]

Chiar dacă obligația de menținere a evidențelor de prelucrare aparține organizației care l-a numit, în practica întâlnită în multe state europene, crearea și menținerea evidențelor de prelucrare este realizată de responsabilul cu protecția datelor în cooperare cu departamentele specializate din cadrul entității în care acționează. Apreciem că astfel de abordare este corectă și poate reprezenta un mijloc util în îndeplinirea sarcinilor specifice de către responsabilul cu protecția datelor, asigurând totodată o evidență unitară a proceselor de prelucrare la nivelul organizației.

Este evident așadar că Regulamentul acordă o importanța sporită responsabilului cu protecția datelor. Fiind chemat să verifice aplicarea normelor incidente în materia protecției datelor cu caracter personal, acesta ar trebui să aibă o abordare bazată pe risc, urmând a se concentra pe acele aspecte ce pot genera riscuri ridicate pentru drepturile persoanelor vizate.

Cu toate acestea, aspectele cu potențial mai scăzut de risc nu pot fi neglijate.

Prin urmare, în activitatea specifică, responsabilul cu protecția datelor trebuie să stabilească o metodologie de lucru pragmatică și selectivă în funcție de nivelurile de risc asociate prelucrărilor de date cu caracter personal.

Sarcinile Responsabilului pentru protectia datelor cu caracter personal (DPO)

1. *Monitorizarea respectării RGPD*

Art. 39(1)b) din Regulament încredințează DPO, printre alte sarcini, obligația de a monitoriza respectarea RGPD.

Considerentul 97 din Regulament precizează în continuare că DPO „ar trebui să acorde asistență operatorului 17 sau persoanei împuternicite de operator pentru monitorizarea conformității cu prezentul Regulament".

Ca parte a acestor sarcini de monitorizare a conformității, DPO poate, în special:

- să colecteze informații pentru a indentifica operațiunilor de prelucrare
- să analizeze și să verifice conformitatea operațiunilor prelucrare
- să informeze, să consilieze și să emită recomandări operatorului sau persoanei împuternicite de operator.[68]

Monitorizarea conformității nu înseamnă că DPO este personal responsabil în situația în care există un caz de nerespectare. Regulamentul spune clar că operatorul, și nu DPO, are obligația de a „pune în aplicare măsuri tehnice șiorgnizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul Regulament" (art. 24(1)).[69]

[67]Cécile de Terwangne, Internet et la protection de la vie privées des données à caractèrepersonnel, în volumul "L'Europe des droits de l'homme à l'heured'Internet" de Quentin van Enis şi Cécile de Terwangne (dir.), Éditions Bruylant, Bruxelles, 2019, p. 325.

[68]Recomandarea CM/Rec (2010) 13 din 23 noiembrie 2010 a Comitetului de Miniștri al Consiliului Europei asupra protecției persoanelor cu privire la prelucrarea automată a datelor cu caracter personal în cadrul creării de profiluri, în Cécile de Terwangne, op. cit., p. 334, inclusiv nota de subsol nr. 34.

[69]C.J.U.E., Marea Cameră, 8 aprilie 2014, Digital RightsIreland, aff. jointes C-293/12 și C-594/12 în ibidem, p. 331, inclusiv nota de subsol nr. 23. Directiva 2006/24/CE a Parlamentului European şi a Consiliului, din 15 martie 2006, publicată în J.O.U.E., L. 105, p. 54.

Respectarea normelor de protecției a datelor este o responsabilitate corporativă a operatorului și nu a DPO.

2. Rolul DPO în evaluarea impactului operațiunilor de prelucrare

Potrivit art. 35(1), operatorul și nu DPO efectuează, atunci când este necesar, o evaluare a impactului operațiunilor de prelucrare („DPIA").

Cu toate acestea, DPO poate avea un rol foarte important și util în asistarea operatorului. Potrivit principiului protecția datelor începând cu momentul conceperii, art. 35(2) prevede în mod expres ca operatorul „să solicite avizul" DPO la realizarea DPIA.

La rândul său, art. 39(1)c) prevede ca și sarcină pentru DPO „să ofere consiliere la cerere în ceea ce privește DPIA și să monitorizese funcționarea acesteia, în conformitate cu art. 35".

Regulamentul recomandă ca operatorul să solicite avizul DPO în legătură cu următoarele aspecte, printre care:

- dacă să efectueze sau nu DPIA
- ce metodologie să fie folosită la efectuarea DPIA
- dacă să efectueze DPIA intern sau să externalizeze
- ce garanții (inclusiv măsuri tehnice și organizaționale) să pună în aplicare pentru reducerea oricăror riscuri la adresa drepturilor și intereselor persoanelor vizate
- dacă DPIA a fost sau nu efectuată corect și dacă respectivele concluzii (dacă să continue sau nu prelucrarea și ce garanții să pună în aplicare) respectă RGPD.

În situația în care operatorul nu este de acord cu opinia DPO, documentația DPIA ar trebui să justifice în mod specific în scris motivul pentru care nu a fost urmat avizul.[70]

Art 39(1) precizează sarcinile DPO și indică faptul că DPO trebuie să aibă „cel puțin" următoarele atribuții. Prin urmare, nimic nu împiedică operatorul să atribuie DPO alte sarcini decât cele menționate în mod expres în art. 39(1) sau să specifice respectivele atribuții întrun mod detaliat.

Art. 24(1) prevede că „ținând seama de natura, domeniul de aplicare, contextul și sopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul Regulament. Respectivele măsuri se revizuiesc și de actualizează dacă este necesar".

3. Cooperarea cu autoritatea de supraveghere și asumarea rolului de punct de contact

Potrivit art. 39(1) d) și c), DPO ar trebui „să coopereze cu autoritatea de supraveghere" și „să-și asume rolul de punct de contact petnru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusive consultarea prealabilă

[70]Avizul nr. 4/2007 emis de Grupul de lucru intemeiat in baza art. 29, pag. 9, exemplul nr. 3, pag. 10, par. 4, pag. 19, exemplul nr. 14, Opinia nr. 8/2001 emisa de Grupul de lucru intemeiat in baza art. 29, pag. 24, Working Document on theProcessing of Personal Data bymeans of Video Surveillance emis de Grupul de lucru intemeiat in baza art. 29, pag. 12.

mențională la art. 36, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune".

Aceste sarcini se referă rolul de „persoană care facilitează" al DPO menționat în cuprinsul intruducerii acestui Ghid. DPO acționează ca punct de contract pentru a facilita accesul autorității de supraveghere la documente și informații pentru îndeplinirea atribuțiilor menționate la art. 57, precum și pentru exercitarea competențelor de investigarea, corectare, autorizare și consultare menționate la art. 58.

Așa cum a fost deja menționat, DPO are obligația de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale, în conformitate cu dreptul Uniuniii sau cu dreptul intern (art. 38(5)).

Cu toate acestea, obligația secretului/confidențialității nu înterzice DPO să contacteze și să solicite consiliere din partea autorității de supraveghere.

Art. 39(1)e) prevede că DPO poate consulta autoritatea de supraveghere cu privire la orice altă chestiune, după caz.[71]

4. Abordare bazată pe risc

Art. 39(2) impune ca DPO „să țină seamă în mod corespunzător de riscul asociat operațiunilor de prelucrare, luând în considerare natura, domeniul de aplicare, contextul și scopurile prelucrării".

Acest articol reamintește de un principiu general și de bun simț care poate fi relevant pentru mai multe aspecte din activitatea zilnică a DPO. În esență, este nevoie ca DPO să prioritizeze activitățile sale și să-și concentreze eforturile asupra problemelor care prezintă riscuri mai mari pentru protecția datelor.

Acest lucru nu înseamnă că ar trebui să-și neglijeze monitorizarea conformității operațiunilor de prelucrare a datelor care au un nivel relativ mai scăzut de risc, ci indică faptul că ar trebui să se concentreze, în primul rând, pe zonele cu risc mai mare.

Această abordare selectivă și pragmatică ar trebui să ajute DPO în consilierea operatorului cu privire la metodologia folosită la efectuarea DPIA, ce zone ar trebui să fac obiectul unui audit intern sau extern privind protecția datelor, ce activități interne de pregătire să fie oferite personalului sau managementului responsabil cu activitățile de prelucrarea și ce operațiuni de prelucrare necesită mai mult timp și resurse.

5. Rolul DPO în păstrarea evidenței

Potrivit art. 30(1) și (2) operatorul sau persoana împuternicită de operator, și nu DPO, are obligația de a „păstra o evidență a operațiunilor de prelucrare desfășurate sub resbonsabilitatea sa" sau de „păstra o evidență a tuturor categoriilor de operațiuni de prelucrare efectuate în numele operatorului".

În practică, DPO crează adesea inventare și deține un registru al operațiunilor de prelucrare pe baza informațiilor furnizate de diferitele departamente din cadrul organizației responsabile cu prelucrarea datelor cu caracter personal.

Această practică a fost stabilită în conformitate cu diverse legislații naționale curente și în conformitate cu normele de protecție a datelor aplicabile instituțiilor și organismelor UE.

[71]Working Document on the Processing of Personal Data bymeans of Video Surveillance emis de Grupul de lucru intemeiat in baza art. 29, pag. 15, 19; Opinion 8/2001 on the processing of personal data in the employment context emis de Grupul de lucru intemeiat in baza art. 29, pag. 25; Guidelines 3/2019 on processing of personal data through video devices emis de Comitetul European pentru Protectia Datelor, pag. 7, 22.

Art. 39(1) prevede o listă minimă a sarcinilor DPO. Prin urmare, nimic nu împiedică operatorul sau persoana împuternicită de operator să atribuie DPO sarcina de a păstra o evidență a operațiunilor de prelucrare în numele operatorului sau persoanei împuternicite de operator.[72]

O astfel de evidență trebuie să fie considerată ca fiind unul dintre instrumentele care permit DPO să-și îndeplinească sarcinile de monitorizare a conformității, informare și consiliere a operatorului sau persoanei împuternicite de operator. În orice caz, evidența păstrată potrivit art. 30 trebuie văzută și ca un instrument care permite operatorului și autorității de supraveghere, la cerere, să aibă o imagine de ansamblu asupra tuturor operațiunile de prelucrare a datelor cu caracter personal efectuate de o organizație. Astfel, este o condiție prealabilă pentru conformitate și, ca atare, o măsură eficientă de responsabilizare.

Pozitia responsabilului cu protecția datelor nu este una foarte clară. Pe de o parte primește responsabilități și sarcini din partea managementului operatorilor și pe de altă parte are responsabilități specifice și se bucură de independență prevazută de GDPR.

Regulamentul European prevede următoarele sarcini:

1. facilitează implementarea politicilor și procedurilor interne în domeniul protecției datelor, precum și instruirea angajaților cu privire la responsabilitățile ce le revin;
2. consilierea personalului și a echipei manageriale în gestionarea incidentelor de securitate a datelor cu caracter personal (ex. abordarea riscurilor de securitate digitală).
3. monitorizarea permanentă a proceselor de prelucrare a datelor desfășurate de operator, identificarea zonelor de îmbunătățire și oferirea de suport în implementarea modificărilor necesare pentru a asigura respectarea celor mai înalte standarde de bune practici în domeniul protecției datelor.
4. analiza solicitărilor venite din partea persoanelor vizate în temeiul RGPD (dreptul de acces, dreptul de a fi uitat, dreptul la rectificarea datelor etc.) și suport în formularea de răspuns.
5. instruirea personalului și a echipei manageriale privind noutățile legislative și bunele practici în domeniul protecției datelor, potrivit specificului activității Operatorului.
6. elaborarea de puncte vedere pe probleme specifice protecției datelor cu caracter personal
7. cooperarea cu autoritatea de control – „Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal”

Obligativitatea desemnării unui DPO

Primul pas pe care un operator trebuie să îl facă este să verifice dacă se află într-o situație care îi impune desemnarea și notificarea unui responsabil cu protecția datelor. Din acest punct de vedere Regulamentul General prevede trei situații în care este obligatorie desemnarea unui DPO:[73]

[72]J. Rochfeld, L’identité numérique en Europe, în E. Pataut (coord.), L’identité à l’épreuve de la mondialisation, Editura Institut de recherche juridique de la Sorbonne, 2016, p.5.
[73]Curtea constituțională federală a Germaniei a statuat în data de 15 decembrie 1983 dreptul la „Informationelle Selbstbestimmung”, adică la „auto-determinare informațională”, apud. J. Rochfeld, L’identité …, p.157.

- reprezentați o autoritate sau un organism public, cu excepția instanțelor care acționează în exercițiul funcţiei lor jurisdicţionale;
- sunteți o companie care desfășoară ca activități principale operațiuni de prelucrare, care, prin natura lor, domeniul de aplicare și/sau scopurile lor, necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă ;
- sunteți o companie care desfășoară activități principale care constau în prelucrarea pe scară largă a unor categorii speciale de date (originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate şi prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viaţa sexuală sau orientarea sexuală ale unei persoane fizice) sau a unor date cu caracter personal privind condamnări penale și infracțiuni;

Decizia de desemnare a responsabilului cu protecția datelor

În cazul autorităților publice, numirea în funcţiile publice pentru care se organizează concurs în condiţiile Legii nr. 188/1999, art. 58 alin. (1) lit. c) (organizat de către autorităţişiinstituţii publice, cu avizul AgenţieiNaţionale a Funcţionarilor Publici, pentru ocuparea funcţiilor publice de execuţie generale şi specifice) se face prin actul administrativ (decizie) emis de conducătorii autorităţilorşiinstituţiilor publice din administraţia publică centrală şi locală care au organizat concursul. Conform art. 62 alin. (4-7) din Legea nr. 188/1999, actul administrativ de numire (decizia) are formă scrisă şi trebuie să conţină temeiul legal al numirii, numele funcţionarului public, denumirea funcţiei publice, data de la care urmează să exercite funcţia publică, drepturile salariale, precum şi locul de desfăşurare a activităţii.

În cazul companiilor private, recomandarea este să existe cel puțin avizul directorului adjunct sau, optim, al directorului general privind adoptarea deciziei de angajare pe postul de DPO, deoarece aceasta semnifică conștientizarea managementului companiei asupra importanței și rolului DPO în cadrul companiei.

Decizia de desemnare a responsabilul cu protecția datelor trebuie să conțină un număr de înregistrare, datele de identificare ale persoanei juridice, temeiul legal pentru desemnarea responsabilului, numele persoanei desemnate.

După desemnarea unui responsabil cu protecția datelor, operatorul are obligația de a notifica ANSPDCP cu privire la acest aspect. Recomandarea noastră este ca datele de contact are DPO-ului să fie unele generice și special atribuite acestei funcții.

Astfel, în eventualitatea schimbării persoanei desemnate, să nu mai fie necesară modificarea acestora pe site, în documentele companiei/instituției, etc.

Modalități de desemnare a responsabilului cu protecția datelor:

- DPO-ul se poate numi fie intern (o persoana deja angajată a operatorului sau o persoană nou angajată) fie extern (angajarea unei persoane special pentru această funcție). Externalizarea funcției de responsabil cu protecția datelor poate fi făcută și către o firmă care oferă astfel de servicii. Acest demers se face printr-un contract de prestări servicii.
- Dacă se numește un DPO intern atunci, în general acest lucru se face prin desemnarea unei persoane prin cumul de funcții. Această numire se face prin modificarea fișei postului prin adăugarea de atribuții și responsabilități specifice.
- Chiar dacă un operator nu se află în situația de a fi obligat să numească un responsabil cu protecția datelor, regulamentul trebuie respectat. În acest caz se

poate desemna intern o persoană, fără a notifica ANSPDCP, care să aibă atribuții în implementarea prevederilor regulamentului gdpr.

Conflictele de interese în desemnarea unui responsabil cu protecția datelor

Atunci când numim un DPO sau Responsabil cu protecția datelor, în primul rând trebuie să avem în vedere conflictul de interese. Dacă responsabilul cu protecția datelor îndeplinește și altă funcție, aceasta din urmă nu trebuie să fie una de conducere. Potrivit art. 38, alin. (3) RGPD, Operatorul se asigură că responsabilul cu protecția datelor nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea acestor sarcini.

Niciun șef de serviciu, compartiment sau membru al echipei manageriale nu poate, în temeiul vreunui regulament intern de organizare și funcționare să dea dispoziții DPO în ceea ce privește exercitarea atribuțiilor sale.

Astfel ar putea apărea situația în care, în calitate de DPO, persoana în cauză ar trebui să analizeze o situație apărută în urma unei decizii luate de aceeași persoană, dar în exercitarea funcției de conducere.

Mai jos vom exemplifica câteva situații în care apare conflictul de interese în numirea unui DPO:

1. Administrator sau director general: apare un conflict de interese general, având în vedere și puterea decizională generală cu privire la activitatea unei societăți.
2. Director financiar: acesta ar putea influența decizia de a aproba finanțarea unor sau a tuturor măsurilor specifice și necesare pentru conformarea cu cerințele stabilite de legislația privind protecția datelor.
3. Director sau șef birou resurse umane: poate să influențeze mecanismele de prelucrare a datelor angajaților, foștilor angajați, sau a potențialilor angajați.
4. Directorul de marketing: poate să influențeze mecanismele de prelucrare a datelor clienților în activitatea de marketing.

Articolul 39 alin. (1), lit. a-e) RGPD prevede explicit un minim al sarcinilor responsabilului cu protecția datelor, însă cu caracter principial și sintetic.
În întocmirea fișei de post veți avea în vedere următoarele aspecte:

1. Responsabilul cu protecția datelor răspunde față de management, conducere;
2. Atribuțiile: Informarea și consilierea, monitorizarea respectării prevederilor Regulamentului, furnizarea de consiliere la cerere, cooperarea cu autoritatea de supraveghere, asumarea rolului de punct de contact pentru autoritatea de supraveghere etc.
3. Responsabilități: păstrează secretul sau confidențialitatea;
4. Implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal;
5. Răspunde de îmbunătățirea permanentă a pregătirii sale profesionale;
6. Folosește timpul de muncă exclusiv pentru îndeplinirea sarcinilor de serviciu.

Pentru asigurarea unei aplicări unitare a Regulamentului General privind Protecția Datelor, Grupul de Lucru Art. 29 de pe lângă Comisia Europeană a emis Ghidul privind Responsabilul cu protecția datelor (DPO).

Cazurile în care este obligatorie desemnarea unui responsabil cu protecția datelor

1. Când prelucrarea este efectuată de o autoritate publică sau un organism public, cu excepția instanțelor care acționează în exercițiul funcției lor jurisdicționale
2. Dacă activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrarea care necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă
3. Dacă activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date sau a unor categorii de date cu caracter personal privind condamnări penale și infracțiuni

Ce înseamnă ”Activități principale”?

Pentru a stabili activitatea principală desfășurată de un operator sau împuternicit, aceasta trebuie analizată prin raportare la prelucrările de date cu caracter personal efectuate.[74]

La ce se referă „Monitorizarea periodică și sistematică”?

Aceasta presupune toate formele de urmărire și profilare pe Internet, inclusiv în scop de publicitate comportamentală, nefiind însă restrictionată în mediul online.

Sintagma ”periodică și sistematică” presupune o activitate continuă și recurentă, care implică prelucrări de date.

Ce presupune prelucrarea ”Pe scară largă”?

Pentru a se stabili dacă o prelucrare este pe scară largă trebuie ținut cont de 4 criterii:

- numărul persoanelor vizate – un număr exact ori un procent din populația relevantă;
- volumul datelor și/sau gama de elemente diferite de date în curs de prelucrare;
- durata sau permanența activității de prelucrare a datelor;
- suprafața geografică a activității de prelucrare.

Ce înseamnă ”Categorii speciale de date”?

Categoriile speciale sunt acele date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice.

Exemple de situații care pot constitui o monitorizare periodică și sistematică a persoanelor vizate:

- gestionarea unei rețele de telecomunicații;

[74]Fr. Zenati-Casting, Th. Revet, Lesbiens, ediția a 3-a, Editura Presses Universitaires de France Droit, Paris 2008, p. 19.

- profilare și scoring în scopul evaluării riscurilor (de exemplu, în scopul acordării unui credit, stabilirea primelor de asigurare, de prevenire a fraudelor, detectarea spălării banilor);
- urmărirea locației, spre exemplu prin aplicații mobile (geolocalizare);
- desfășurarea de programe de loialitate;
- monitorizarea stării de sănătate prin intermediul dispozitivelor portabile;
- televiziune cu circuit închis – CCTV;
- prelucrarea datelor pacienților de către un spital;
- prelucrarea datelor datelor de conținut, locație, trafic de către furnizorii de servicii de internet;
- prelucrarea datelor personale de către companii de asigurări;
- publicitate comportamentală.

Când nu este necesară desemnarea unui responsabil cu protecţia datelor?

– Atunci când nu se prelucrează pe scară largă date cu caracter personal.

Spre exemplu:

- prelucrarea datelor pacientului de către un cabinet medical individual;
- prelucrarea datelor personale referitoare la condamnările penale și infracțiuni de către un cabinet individual de avocatură.

De reținut !

Deși în unele cazuri nu este necesară desemnarea unui responsabil cu protecția datelor, Autoritatea de Supraveghere recomandă numirea unei astfel de persoane, întrucât este utilă operatorului pentru respectarea obligațiilor în domeniul protecției datelor cu caracter personal.

Cine poate îndeplini funcția de responsabil cu protecția datelor?

Articolul 37 alin. 5 din Regulamentul UE 2016/679 stabilește ca responsabilul cu protecția datelor să fie ”desemnat pe baza calităților profesionale și, în special, a cunoștințelor de specialitate în dreptul și practicile din domeniul protecției datelor, precum și pe baza capacității de a îndeplini sarcinile prevăzute la articolul 39.”[75]

Responsabilul cu protecția datelor poate fi angajat al operatorului/persoanei împuternicite de operator sau poate să-și îndeplinească sarcinile pe baza unui contract de prestări servicii.

[75]Hotărârea CEDO din 7 februarie 2012 în cauza Von Hannover/Germania (nr. 2) [T], nr. 40660/08 și 60641/08; Hotărârea CJUE din 24 noiembrie 2011 în cauzele conexate C-468/10 și C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) și Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado, punctul 48; Hotărârea CJUE din 29 ianuarie 2008 în cauza Productores de Música de España (Promusicae)/Telefónica de España

În domeniul public, poate fi desemnat pentru mai multe autorități sau instituții publice, luând în considerare structura organizatorică și dimensiunea acestora.

Principala preocupare a responsabilului cu protecția datelor trebuie să fie respectarea Regulamentului General privind Protecția Datelor și a reglementărilor naționale incidente.

Este obligat să păstreze secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale, în conformitate cu dreptul Uniunii sau cu dreptul intern.
Operatorul sau persoana împuternicită de operator, în ceea ce privește raporturile cu responsabilul cu protecția datelor, este obligat să:

- publice datele de contact ale responsabilului (adresă poștală, număr de telefon alocat special și/sau o adresă de email alocată special).
- comunice datele de contact ale responsabilului către Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

Responsabilului cu protecția datelor îi este permis să aibă și alte funcții.
Acestuia îi pot fi încredințate și alte sarcini și atribuții, cu condiția ca acestea să nu dea naștere unor conflicte de interese (de ex: nu poate fi director executiv, director operațional, director financiar, șeful serviciului medical, șeful departamentului de marketing, șeful departamentului de resurse umane sau șeful departamentului IT).
Responsabilul pentru protecția datelor nu poate fi demis sau sancționat de operator sau persoana împuternicită de operator pentru îndeplinirea sarcinilor sale.
De exemplu, responsabilul nu poate fi demis pentru oferirea unui sfat conform sacinilor sale.
Un responsabil cu protecția datelor ar putea fi totuși demis, în mod legal, din alte motive decât cele privind îndeplinirea sarcinilor sale în această calitate.
De exemplu, responsabilul poate fi demis în caz de furt, hărțuire ori o abatere gravă similară.[76]

Sarcinile responsabilului cu protecția datelor

- de a informa şi consilia operatorul, sau persoana împuternicită de operator, precum şiangajaţii care se ocupă de prelucrările de date;
- de a monitoriza respectarea Regulamentului, a altor dispoziţii de drept al Uniunii sau de drept intern referitoare la protecţia datelor;
- de a consilia operatorul în ceea ce priveşte realizarea unei analize de impact asupra protecţiei datelor şi de a monitoriza executarea acesteia;
- de a coopera cu Autoritatea de Supraveghere și de a reprezenta punctul de contact cu aceasta;
- de a ține seama în mod corespunzător de riscul asociat operațiunilor de prelucrare, la îndeplinirea sarcinilor sale.

Responsabilul cu protecția datelor personale este acea persoană desemnată de operator sau de către persoana împuternicită de acesta cu scopul de a implementa

[76]Consiliul Europei, Comitetul consultativ al Convenției 108, Orientări privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal într-o lume a datelor masive, 23 ianuarie 2017, p. 2; Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor, intitulată „Către o economie de succes bazată pe date", COM(2014) 442 final din 2 iulie 2014, Bruxelles, p. 4; Recomandarea Y.3600 din 2015 a Uniunii Internaționale a Telecomunicațiilor, intitulată „Big Data – Cloud computing based requirements and capabilities" (Datele masive – cerințe și capabilități bazate pe tehnologia de tip cloudcomputing)

proceduri care validează respectarea prezentului Regulament și de a superviza persoanele care prelucrează date cu caracter personal.

Articolul 37 alin. 1 din Regulament expune cazurile în care operatorul are obligația de a desemna un responsabil.
Responsabilul este desemnat:

1. *Când prelucrarea este efectuată de o autoritate sau organism public, cu excepția instanțelor care acționează în exercițiul funcției lor jurisdicționale;*
2. *Când activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrare, care, prin natura, domeniul de aplicare și/sau scopurile lor, necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă;*
3. *Când activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date, sau a unor date cu caracter personal privind condamnări penale și infracțiuni.*

Responsabilul cu prelucrarea datelor personale este desemnat pe baza calităților profesionale și a cunoștințelor de specialitate în dreptul și practicile din domeniul protecției datelor, precum și pe baza capacității de a îndeplini obligațiile prevăzute la articolul 39.[77]

Sarcinile responsabilului cu protecția datelor prevăzute de articolul 39

Persoana desemnată cu protecția datelor are următoarele obligații:

1. Să informeze și să consilieze operatorul, persoana desemnată de operator să prelucreze date, precum și angajații care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul respectării regulamentului și al altor dispoziții de drept al Uniunii sau dreptului intern cu privire la protecția datelor;
2. Să monitorizeze respectarea prezentului regulament, a altor dispoziții de drept al Uniunii sau de drept intern cu referire la protecția datelor inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului desemnat cu operațiunile de prelucrare, precum și auditurile aferente;
3. Să furnizeze consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia;
4. Să coopereze cu autoritatea de supraveghere;
5. Să-și asume rolul de persoană de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare inclusiv consultarea prealabilă în ceea ce privește evaluarea impactului asupra protecției datelor, precum și cu privire la orice alte chestiuni;

Responsabilul cu protecția datelor ține seama în mod corespunzător de riscul asociat operațiunilor de prelucrare, luând în calcul natura, domeniul de aplicare, contextul și scopurile pentru care se prelucrează date personale.

Pentru a îndruma modul în care sunt gestionate datele cu caracter personal în cadrul unui operator sau al unei persoane împuternicite de operator, în anumite situații, este necesară o persoană care să exercite o misiune de informare, de consiliere și de control în plan intern: responsabilul cu protecția datelor.

[77]Hotărârea CJUE [MC] din 8 aprilie 2014 în cauzele conexate C-293/12 și C-594/12, Digital RightsIreland Ltd/Minister for Communications, Marine and Natural Resources și alții și Kärntner Landes regierung și alții, punctul 69.

Poate fi numit responsabil cu protecția datelor, cineva din afara firmei sau poate fi un angajat al firmei. Este necesar să fie un specialist în protecția datelor și trebuie să rămână independent în activitatea pe care o desfășoară și nu trebuie să aibă un alt rol cheie în prelucrarea datelor personale din companie, pentru a nu fi în incompatibilitate.

Desemnarea unui responsabil cu protecţia datelor este obligatorie potrivit GDPR, în cazul în care operatorul sau persoana împuternicită de operator: este o autoritate publică sau un organism public, cu excepţiainstanţelor în exercitarea funcţiei lor jurisdicţionale; desfășoară o activitate principală care conduce la realizarea unei monitorizări constante și sistematice pe scară largă a persoanelor; desfășoară o activitate principală care constă în prelucrarea pe scară largă de date sensibile (cum ar fi : date privind originea rasială sau etnică, convingerile religioase, apartenența sindicală, date genetice, biometrice, privind starea de sănătate).

La ce ajută numirea unui responsabil cu protecția datelor, când aceasta nu este obligatorie?

Chiar dacă entitatea nu are obligaţia expresă de a desemna un responsabil cu protecția datelor, ANSPDCP recomandă numirea acestuia, în considerarea efectului benefic al activităţii responsabilului în vederea asigurării respectării Regulamentului General de Protecţia Datelor de către operatorul respectiv sau persoana împuternicită de operator.

Un responsabil cu protecția datelor reprezintă un avantaj major pentru operator în vederea înţelegerii și respectării obligaţiilor prevăzute de GDPR, dialogului cu autoritățile pentru protecția datelor și reducerii riscurilor apariţiei unor litigii.

Rolul responsabilului cu protecţia datelor să informeze și să consilieze operatorul sau persoana împuternicită de operator, precum și angajaţii acestora cu privire la obligaţiile existente în domeniul protecţiei datelor cu caracter personal; să monitorizeze respectarea GDPR și a legislaţieinaţionale în domeniul protecţiei datelor; să consilieze operatorul sau persoana împuternicită în legătură cu realizarea de studii de impact privind protecția datelor și să verifice efectuarea acestora; să coopereze cu autoritatea pentru protecţia datelor și să reprezinte punctul de contact în relaţia cu aceasta.

Toţi operatorii din sistemul public, persoanele împuternicite de operator, precum și operatorii din sistemul privat cu peste 250 de angajaţi, au obligaţia cartografierii prelucrărilor de date cu caracter personal efectuate.

Chiar și operatorii din sistemul privat cu mai puţin de 250 de angajaţi au obligaţia cartografierii prelucrărilor în cazurile în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertăţile persoanelor vizate.

Pentru a evalua în mod eficient impactul GDPR asupra activităţii dv. de business și a societății comerciale, este necesară identificarea prelucrărilor de date cu caracter personal efectuate și păstrarea evidenţeiactivităţilor de prelucrare.

Pentru a avea o evidență completă și exactă a prelucrărilor de date cu caracter personal efectuate și pentru a răspunde noilor exigenţe, trebuie identificate, în prealabil, cu precizie: diferitele prelucrări de date cu caracter personal; categoriile de date cu caracter personal prelucrate; scopurile urmărite prin operaţiunile de prelucrare a datelor; persoanele care prelucrează aceste date; fluxurile de date, indicând originea și destinația datelor.

CAP IV. RELAȚIA CU AUTORITATEA DE SUPRAVEGHERE ÎN DOMENIUL PROTECȚIEI DATELOR CU CARACTER PERSONAL ȘI ROLUL PUNCTULUI DE CONTACT

Instituirea în statele membre a unor autorități de supraveghere, împuternicite să își îndeplinească sarcinile și să își exercite competențele în deplină independență, este un element esențial al protecției persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal. Statele membre ar trebui să poată institui mai multe autorități de supraveghere, pentru a reflecta structura lor constituțională, organizatorică și administrativă.[78]

Independența autorităților de supraveghere nu ar trebui să însemne că autoritățile de supraveghere nu pot face obiectul unor mecanisme de control sau de monitorizare în ceea ce privește cheltuielile acestora sau unui control jurisdicțional.

În cazul în care un stat membru instituie mai multe autorități de supraveghere, acesta ar trebui să stabilească prin lege mecanisme care să asigure participarea efectivă a autorităților de supraveghere respective la mecanismul pentru asigurarea coerenței. Statul membru respectiv ar trebui, în special, să desemneze autoritatea de supraveghere care îndeplinește funcția de punct unic de contact pentru participarea efectivă a acestor autorități la mecanism, în scopul asigurării unei cooperări rapide și armonioase cu alte autorități de supraveghere, cu comitetul și cu Comisia.

Fiecare stat membru se asigură că una sau mai multe autorități publice independente sunt responsabile de monitorizarea aplicării prezentului regulament, în vederea protejării drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea și în vederea facilitării liberei circulații a datelor cu caracter personal în cadrul Uniunii ("autoritatea de supraveghere").

Fiecare autoritate de supraveghere contribuie la aplicarea coerentă a prezentului regulament în întreaga Uniune. În acest scop, autoritățile de supraveghere cooperează atât între ele, cât și cu Comisia.[79]

În cazul în care mai multe autorități de supraveghere sunt instituite într-un stat membru, acesta desemnează autoritatea de supraveghere care reprezintă autoritățile respective în cadrul comitetului și instituie un mecanism prin care să asigure respectarea de către celelalte autorități a normelor privind mecanismul pentru asigurarea coerenței.

Fiecare stat membru notifică Comisiei dispozițiile de drept pe care le adoptă în temeiul prezentului capitol până la 25 mai 2018 și, fără întârziere, orice modificare ulterioară pe care o aduce acestor dispoziții.

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

---

[78]Voroneanu Carmen, Aspecte de ordin practic privind implementarea cerințelor "Regulamentului general privind protecția datelor" (RGPD) în biblioteci, An 32Nr. 52021p. 23-28https://www.bibnat.ro/dyn-doc/publicatii/Revista Biblioteca 5_2021_site.pdf

[79]Sava, Ruxandra, Regulamentul General privind Protecţia Datelor (RGPD) pe înţelesul tău, Bucureşti Editură Universul Juridic, 2019, pag. 221

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.[80]

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.

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.

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.

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.

Obiectivele esențiale ale strategiei privind activitatea Autoritatii Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal sunt întărirea capacității instituționale a autorității de supraveghere, îmbunătățirea nivelului de conștientizare a obligațiilor operatorilor de date personale, precum și a drepturilor persoanelor vizate.

În subsidiar, se urmarește eficientizarea capacității administrative a instituției, îmbunătățirea informării publice prin elaborarea, editarea și difuzarea de materiale informative, aplicarea dispozițiilor legislației în materie de protecție a datelor cu caracter personal și, nu în ultimul rand, creșterea numărului de investigații și aplicarea de sancțiuni în cazul nerespectării prevederilor legale. [81]

Autoritatea Nationala de Supraveghere, se afla în prezent într-un amplu proces de reformă ca urmare a intrarii in vigoare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date si de abrogare a Directivei 95/46/EC (Regulamentul general privind protecția datelor), publicat in Jurnalul Oficial al Uniunii Europene nr. L 119 din 4 mai 2016, act normativ de directa aplicare în toate statele membre începând cu data de 25 mai 2018.

În considerarea noilor reglementări adoptate recent la nivelul Uniunii Europene și a celorlalte competente stabilite prin actele normative menționate mai sus, a fost adoptată de Parlamentul Romaniei Legea nr. 129 din 15 iunie 2018 pentru modificarea și completarea Legii nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum

[80]Luncaşu, Silviu-Cristian, Formarea şi dezvoltarea pregătirii responsabilului cu protecţia datelor cu caracter personal (DPO), în lumina noului GDPR (UE) nr. 679/2016, Bucureşti, Editură Edit Moroşan, 2018, pag. 95

[81]Giurgiu, Andra, Protecţia datelor cu caracter personal din perspectiva dreptului european, Teza de Doctorat,niversitatea "Lucian Blaga" din Sibiu. Facultatea de Drept. Şcoala Doctorală, 2013, pag. 155

și pentru pag.3 abrogarea Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.[82]

Este de observat că dispozițiile Regulamentului general privind protecția datelor, în special celeale art. 55-59, extind competențele și sarcinile de monitorizare și control ale autorităților naționale de supraveghere a prelucrarii datelor cu caracter personal și, implicit, ale Autorității Naționale de Supraveghere. Astfel, statele membre ale Uniunii Europene au obligația de a asigura resursele adecvate autorităților pentru protecția datelor personale, potrivit art. 52 din Regulamentul (UE) 2016/679: ”(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 efectiva a competentelor sale, inclusiv a celor care urmeaza să fie aplicate în contextul asistentei reciproce, al cooperarii și al participării în cadrul comitetului.

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

Luând în considerare că prevederile Regulamentului (UE) 2016/679 se aplica direct în toate statele membre, aceasta presupune dotarea corespunzatoare cu resurse materiale ăi umane în mod uniform, a tuturor autorităților naționale de supraveghere. În acest sens, chiar Comisarul european pentru justiție, consumatori și egalitate de gen, a adresat, la data de 24 mai 2017, Președiției malteze a Uniunii Europene, o scrisoare în care sublinia necesitatea de a se oferi autorităților lornationale de supraveghere resurse financiare și umane suficiente în vederea exercitării atribuțiilor.[83] În acest context, subliniem că Autoritatea Națională de Supraveghere este autoritate centrala unică la nivel național și nu are în organizarea sa structuri teritoriale.

În plus, Regulamentul privind respectarea vieții private și protecția datelor cu caracter personal în comunicațiile electronice și de abrogare a Directivei 2002/58/CE (Regulamentul privind viața privata și comunicațiile electronice) menționează că responsabilitatea verificăriirespectarii normelor de confidențialitate prevăzute în acest regulament revine autorităților naționale de supraveghere, începand cu data de 25 mai 2018, în concordanță cu Regulamentul (UE) 2016/679.

În același timp, propunerea de Regulament de instituire a Sistemului de intrare/ieșire (EES) pentru înregistrarea datelor de intrare și de ieșire și a datelor referitoare la refuzul intrării în ceea ce îi privește pe resortisantii țărilor terțe care trec frontierele externe ale statelor membre ale Uniunii Europene, de stabilire a condițiilor de acces la EES în scopul asigurării respectarii legii și de modificare a Regulamentului (CE) nr. 767/2008 și a Regulamentului (UE) nr. 1077/2011 (propunere ce urmează a fi adoptată în cursul anului 2017) prevede ca autoritățile naționale de supraveghere vor fi responsabile de supravegherea prelucrării datelor din acest sistem, ale cetățenilor țărilor terțe.

De asemenea, propunerea de Regulament al Parlamentului European și al Consiliului de instituire a Sistemului european de informații și de autorizare privind călătoriile (ETIAS) și de modificare a Regulamentelor (UE) nr. 515/2014, (UE) 2016/399, (UE) 2016/794 și (UE) 2016/1624 prevede ca și în cazul acestui sistem autoritatea

[82]Daniel – Mihail Șandru, Imposibila coexistență între protecția datelor și comunitățile virtuale? Ce urmează?, Pandectele Române nr. 1/2018, p. 18.
[83]Ruxandra Sava, Când decizia o ia mașina… Despre profilare, drepturi și echilibru într-un univers digital, Revista Romana pentru Protecția și Securitatea Datelor cu Caracter Personal nr. 3/2020, p. 24-41.

națională de supraveghere instituita în conformitate cu Regulamentul (UE) 2016/679 ar trebui să monitorizeze legalitatea prelucrării datelor cu caracter personal de catre statele membre.

Mai mult, în prezent, Autoritatea Națională de Supraveghere are competențe de control și în următoarele domenii de activitate, potrivit actelor normative ce le reglementeaza, astfel:[84]

- în domeniul comunicațiilor electronice, acordate prin Legea nr. 506/2004 privind protecția vieții private în domeniul comunicațiilor electronice, modificată și completată prin Ordonanța de urgența a Guvernului nr. 13/2012 adoptată pentru implementarea prevederilor Directivei 2009/136/EC a Parlamentului European și a Consiliului;

- în privintanotificărilor încălcărilor de securitate, potrivit Regulamentul 611/2013/EC privind măsurile aplicabile notificărilor încălcărilor securității datelor cu caracter personal în temeiul Directivei 2002/58/EC a Parlamentului și a Consiliului privind confidențialitatea și comunicațiile electronice, prin care se stabilesc condițiile și formatul notificărilor încălcărilor de securitate ce se transmit de operatorii de date catre autoritățile naționale de protecție a datelor personale din statele membre ale Uniunii Europene;

- în domeniul reglementat de Legea nr. 141/2010 privind înființarea, organizarea și funcționarea Sistemului Informatic Național de Semnalări și participarea României la Sistemul de Informații Schengen;

- în domeniul vizelor, potrivit Legii nr. 271/2010 privind înființarea, organizarea și funcționarea Sistemului național de informații privind vizele și participarea României la Sistemul de informații privind vizele.

Politica publică specifică a Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal consta în realizarea programului de aparare a drepturilor și libertăților persoanelor fizice cu privire la prelucrarea datelor cu caracter personal și liberă circulație a acestor date.

În conformitate cu prevederile Regulamentului nr. 679 din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor), publicat în Jurnalul Oficial al Uniunii Europene, seria L, nr. 119 din 4 mai 2016, denumit în continuare Regulamentul general privind protecția datelor, autoritatea națională de protecția datelor este responsabilă de monitorizarea aplicării prezentului regulament, în vederea protejării drepturilor și

[84]De exemplu, în cauza C-136/17, GC și alții (Lizibilitatea datelor sensibile), hotărârea din 24 septembrie 2019. ECLI:EU:C:2019:773, pct. 44, CJUE a arătat că datele speciale necesită o protecție sporită deoarece sunt susceptibile să constituie o ingerință deosebit de gravă în drepturile de la art. 7 și 8 din Cartă; În cauza Google Spain (CJUE, C-131/12, Google Spain și Google, hotărârea din 13 mai 2014 ECLI:EU:C:2014:317), CJUE a arătat că, în exercițiul de ponderare a dreptului la protecția datelor cu libertatea de exprimare și informare, se ține cont și de gradul ingerinței în drepturile persoanei vizate. În cauza Digital RightsIreland (hotărârea din 8 aprilie 2014 , ECLI:EU:C:2014:238, pct. 37), un argument care a contribuit la invalidarea Directivei 2006/2004 a fost acela că datele pe care trebuiau să le păstreze furnizorii de servicii de telecomunicații „pot permite deducerea unor concluzii foarte precise privind viața privată a persoanelor ale căror date au fost păstrate, precum obiceiurile din viața cotidiană, locurile de ședere permanente sau temporare, deplasările zilnice sau alte deplasări, activitățile desfășurate, relațiile sociale ale acestor persoane și mediile sociale frecventate de ele”.

libertăţilor fundamentale ale persoanelor fizice în ceea ce priveşte prelucrarea şi în vederea facilitării liberei circulaţii a datelor cu caracter personal în cadrul Uniunii.[85]

Fiecare autoritate de supraveghere beneficiază de independenţă deplină în îndeplinirea sarcinilor sale şi exercitarea competenţelor sale în conformitate cu prezentul regulament.

Totodată, conducerea fiecărei autorităţi de supraveghere, în cadrul îndeplinirii sarcinilor şi al exercitării competenţelor sale în conformitate cu prezentul regulament, rămâne independentă de orice influenţă externă directă sau indirectă şi nici nu solicită, nici nu acceptă instrucţiuni de la o parte externă.

Aplicarea, pe data de 25 mai 2018, a Regulamentului general privind protecția datelor a condus la necesitatea armonizării prevederilor naționale care reglementau domeniul protecției datelor cu caracter personal cu dispozițiile acestui act normativ european.[86]

În acest context, prin Legea nr. 129/2018 de modificare și completare a Legii nr. 102/005 privind înființarea, organizarea şifuncţionareaAutorităţiiNaţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal s-a urmărit, în principal, asigurarea competențelor și sarcinilor de monitorizare și control ale Autorității Naționale de Supraveghere în acord cu prevederile art. 55-59 din Regulamentul (UE) 2016/679, asigurând în acest mod un cadru legal adecvat pentru respectarea drepturilor specifice ale persoanelor fizice în domeniul prelucrării datelor cu caracter personal (dreptul de informare, dreptul de acces, dreptul la rectificare, dreptul la restricționarea prelucrării, dreptul la ștergerea datelor – dreptul ”de a fi uitat”, dreptul de opoziție, dreptul la portabilitatea datelor), precum și o interacțiune eficientă în relația administrație-cetățeni.

Autoritatea Naţională de Supraveghere are drept obiectiv apărarea drepturilor şilibertăţilor fundamentale ale persoanelor fizice, în special a dreptului la viaţă privată, în legătură cu prelucrarea datelor cu caracter personal şi cu libera circulaţie a acestor date.

Printre principalele atribuţii ale AutorităţiiNaţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal și ale președintelui acesteia, stabilite în acord cu elementele de noutate aduse de Regulamentul (UE) 2016/679, enumerăm:

- monitorizarea aplicării unitare a legislației privind protecția datelor cu caracter personal, de către toate entitățile care au calitatea de operatori de date;

- reglementarea, prin elaborarea de decizii și instrucțiuni cu caracter obligatoriu, care se publică în Monitorul Oficial al României;

- avizarea proiectelor de acte normative în materie de protecție a datelor cu caracter personal;

- îndrumarea, prin activitatea de consiliere, inclusiv a Parlamentului, Guvernului și altor autorități sau instituții publice și a entităților ce au calitatea de operatori de date, precum și informarea persoanelor vizate și a publicului asupra a obligațiilor ce le revin

[85]Steve Peers, Tamara Hervey, JeffKenner, Angela Ward (eds.), The EU Charter of Fundamental Rights: A Commentary, Ed. Beck/Hart, 2014, Marea Britanie, republicată în 2019, p. 238.
[86]Sian Rudgard, Origins and Historical Context of Data Protection Law în lucrarea Eduardo Ustaran, Hogan Lovells (eds.), European Data Protection Law and Practice, International Association of Privacy Professionals (IAPP), 2018, p. 23.

în temeiul legislației în domeniul protecției datelor personale, respectiv drepturilor garantate de lege;

- controlul îndeplinirii obligațiilor legale de către operatorii de date cu caracter personal, prin intermediul competențelor de investigare a încălcării drepturilor persoanelor vizate, din oficiu sau la primirea unei plângeri ori sesizări;

- aplicarea măsurilor corective în situațiile în care se constată încălcări ale legislației în domeniu;

- cooperare și asistență reciprocă cu autoritățile de supraveghere din celelalte state membre, precum și de cooperare cu Comisia Europeană și Comitetul european pentru protecția datelor, în cadrul mecanismului de asigurare a coerenței aplicării Regulamentului general pentru protecția datelor pe teritoriul întregii Uniuni;

- informare a Parlamentului, Guvernului, Comisiei europene și a Comitetului european pentru protecția datelor, asupra activităţii proprii, prin intermediul raportului anual de activitate.

În totalitatea țărilor membre ale Uniunii Europene a fost remarcată de-a lungul timpului, odată cu dezvoltarea sistemului informatic, importanța existenței unei activități de protecție a datelor cu caracter personal. Din acest considerent, au fost constituite organe competente pentru îndeplinirea unor astfel de atribuții. În vederea alinierii legislației române la acquis-ulunional, de la data de 12 mai 2005 intră în vigoare Legea nr.102/2005, prin care se înființează Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.Acest organ reprezintă o autoritate publică centrală autonomă cu competență generală în domeniul protecției datelor personale, fiind garantul respectării drepturilor fundamentale la viață privată și la protecția datelor personale.[87]

Articolele 7 si 8 din Carta Drepturilor Fundamentale a Uniunii Europene, articolul 16 din Tratatul privind Funcționarea Uniunii Europene și articolul 8 din Convenția Europeană pentru Apărarea Drepturilor Omului și Libertăților Fundamentale sunt cele care statuează aceste principii, de altfel de nelipsit dintr-o lume și o societate civilizată, a anului 2018.

Un moment important în evoluția reglementărilor europene cu referire la protecția datelor personale reprezintă anul 2016, în timpul căruia Parlamentul European și Consiliul European adoptă Regulamentul General privind protecția persoanelor fizice în ceea ce presupune prelucrarea datelor cu caracter personal și libera circulație a acestora. Acest regulament are aplicabilitate directa în întregimea statelor Uniunii Europene începand cu data de 25 mai 2018, împreună cu Directiva vizând același subiect, în scopul prevenirii, detectării, investigării și punerii sub urmarire a infracțiunilor și a altor activități judiciare.[88]

---

[87]Carlo Ratti, Dirk Helbing, The Hidden Danger of Big Data în Dirk Helbing, Towards Digital Enlightenment. Essays on the Dark and Light Sides of the Digital Revolution, Ed. Springer, 2019, p. 22.

[88] Decizia civila nr. 34/09.03.2017 a Curții de Apel București, Secția a VIII-a Contencios Administrativ și Fiscal (nepublicată), s-a statuat, în mod definitiv, faptul că adresele de e-mail a căror denumire cuprinde numele, prenumele și locul de muncă al unei persoane (de exemplu, ion.ionescu@companie.ro), reprezintă informații ce servesc la identificarea persoanei fizice, respectiv sunt date cu caracter personal în sensul reglementat de art. 3 lit. a) din Legea nr. 677/2001, articol disponibil pehttps://www.juridice.ro/596856/hotarare-de-impact-a-curtii-de-apel-bucuresti-in-domeniul-protectiei-datelor-cu-caracter-personal-cu-privire-la-obligatiile-angajatorilor-de-gestionare-a-adreselor-de-e-mail-ale-angajatilor-ulterior.html

Așadar, Autoritatea este însărcinată cu monitorizarea si controlul sub aspectul legalității prelucrărilor de date cu caracter personal care cad sub incidența Legii nr. 677/2001. În acest scop, se exercită urmatoarele atribuții:

- ✓ Primește și analizează notificările privind prelucrarea datelor cu caracter personal;
- ✓ Autorizează prelucrările de date în situațiile prevăzute de lege;
- ✓ Poate dispune, în cazul în care constată încălcarea dispozițiilor prezentei legi, suspendarea provizorie sau încetarea prelucrării datelor, ștergerea parțială sau integrală a datelor prelucrate și poate să sesizeze organele de urmărire penală sau să intenteze acțiuni în justiție;
- ✓ Informează persoanele fizice și/sau juridice asupra necesității respectării obligațiilor și îndeplinirii procedurilor prevăzute de Legea nr.667/2001;
- ✓ Păstrează și pune la dispoziția publicului registrul de evidență a prelucrărilor de date cu caracter personal;
- ✓ Primește și soluționează plângeri, sesizări sau cereri de la persoanele fizice și comunică soluția dată sau, după caz, demersurile efectuate;
- ✓ Efectuează controale prealabile în situația în care operatorul prelucrează date cu caracter personal care sunt susceptibile de a prezenta riscuri speciale pentru drepturile și libertățile persoanelor;
- ✓ Efectuează investigații din oficiu sau la primirea unor plângeri sau sesizări;
- ✓ Este consultată atunci când se elaborează proiecte de acte normative referitoare la protecția drepturilor și libertăților persoanelor, în privința prelucrării datelor cu caracter personal;
- ✓ Poate face propuneri privind inițierea unor proiecte de acte normative sau modificarea actelor normative în vigoare in domenii legate de prelucrarea datelor cu caracter personal;
- ✓ Cooperează cu autoritățile publice, centralizează și analizează rapoartele anuale de activitate ale acestora privind protecția persoanelor în privința prelucrării datelor cu caracter personal;
- ✓ Formulează recomandări și avize asupra oricărei chestiuni legate de protecția drepturilor și libertăților fundamentale în privința prelucrării datelor cu caracter personal, la cererea oricărei persoane, inclusiv a autorităților publice și a organelor administrației publice;
- ✓ Cooperează cu autoritățile similare din străinătate, în vederea asistenței mutuale, precum și cu persoanele cu domiciliul sau cu sediul în străinătate, in scopul apărării drepturilor și libertăților fundamentale ce pot fi afectate prin prelucrarea datelor cu caracter personal;
- ✓ Îndeplinește alte atribuții prevăzute de lege.

Articolul 37 alineatul (1) literele (b) și (c) din Regulament vizează „activitățile principale ale operatorului sau ale persoanei împuternicite de operator”. Activitățile principale ale unui operator se referă la „activitățile sale de bază, și nu la prelucrarea datelor cu caracter personal drept activități auxiliare”.

„Activitățile principale” pot fi considerate drept operațiunile-cheie necesare pentru îndeplinirea obiectivelor operatorului sau ale persoanei împuternicite de către operator. Cu toate acestea, „activitățile principale” nu ar trebui să fie interpretate ca excluzând activitățile în cazul în care prelucrarea datelor constituie o parte indisolubilă a activității operatorului sau a persoanei împuternicite de către operator.

De exemplu, activitatea principală a unui spital este de a furniza asistență medicală. Cu toate acestea, spitalul nu ar putea furniza asistență medicală în condiții de

siguranță și în mod eficient, fără prelucrarea datelor privind starea de sănătate, cum ar fi dosarele medicale ale pacienților.

Prin urmare, prelucrarea acestor date ar trebui să fie considerată drept una dintre activitățile principale ale oricărui spital, iar spitalele trebuie, prin urmare, să numească RPD. Într-un alt exemplu, o societate privată de securitate supraveghează o serie de centre comerciale private și spații publice. Supravegherea este activitatea principală a societății, care, la rândul său, este legată în mod indisolubil de prelucrarea datelor cu caracter personal.

Prin urmare, această societate trebuie, de asemenea, să numească un Responsabil pentru protectia datelor. Pe de altă parte, toate organizațiile desfășoară anumite activități, de exemplu, își plătesc angajații sau desfășoară activități standard de asistență IT. Acestea sunt exemple de funcții de asistență necesare pentru activitatea principală sau obiectul principal de activitate al organizației. Chiar dacă aceste activități sunt necesare sau esențiale, acestea sunt considerate, de regulă, ca fiind funcții auxiliare, nu activitatea principală. [89]

În cazul în care prelucrarea este efectuată de o autoritate publică, cu excepția instanțelor sau a autorităților judiciare independente atunci când acționează în calitatea lor judiciară, în cazul în care, în sectorul privat, prelucrarea este efectuată de un operator a cărui activitate principală constă în operațiuni de prelucrare care necesită o monitorizare regulată și sistematică a persoanelor vizate pe scară largă, sau în cazul în care activitatea principală a operatorului sau a persoanei împuternicite de operator constă în prelucrarea pe scară largă de categorii speciale de date cu caracter personal și de date privind condamnările penale și infracțiunile, o persoană care deține cunoștințe de specialitate în materie de legislație și practici privind protecția datelor ar trebui să acorde asistență operatorului sau persoanei împuternicite de operator pentru monitorizarea conformității, la nivel intern, cu prezentul regulament.

În sectorul privat, activitățile principale ale unui operator se referă la activitățile sale de bază, și nu la prelucrarea datelor cu caracter personal drept activități auxiliare. Nivelul necesar al cunoștințelor de specialitate ar trebui să fie stabilit în special în funcție de operațiunile de prelucrare a datelor efectuate și de nivelul de protecție impus pentru datele cu caracter personal prelucrate de operator sau de persoana împuternicită de operator. Acești responsabili cu protecția datelor, indiferent dacă sunt sau nu angajați ai operatorului, ar trebui să fie în măsură să își îndeplinească atribuțiile și sarcinile în mod independent.

Având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal. O evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare.

La realizarea unei evaluări a impactului asupra protecției datelor, operatorul solicită avizul responsabilului cu protecția datelor, dacă acesta a fost desemnat.

[89]Andrei SĂVESCU, Clasificarea operatorilor de date cu caracter personal, articol disponibil pe https://www.juridice.ro/595901/clasificarea-operatorilor-de-date-cu-caracter-personal.html

Evaluarea impactului asupra protecției datelor se impune mai ales în cazul:

(a) unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

(b) prelucrării pe scară largă a unor categorii speciale de date, sau a unor date cu caracter personal privind condamnări penale și infracțiuni,

(c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.

Autoritatea de supraveghere întocmește și publică o listă a tipurilor de operațiuni de prelucrare care fac obiectul cerinței de efectuare a unei evaluări a impactului asupra protecției datelor. Autoritatea de supraveghere comunică aceste liste catre comitet.

Autoritatea de supraveghere poate, de asemenea, să stabilească și să pună la dispoziția publicului o listă a tipurilor de operațiuni de prelucrare pentru care nu este necesară o evaluare a impactului asupra protecției datelor. Autoritatea de supraveghere comunică aceste liste comitetului.[90]

Înainte de adoptarea listelor, autoritatea de supraveghere competentă aplică mecanismul pentru asigurarea coerenței menționat la articolul 63 în cazul în care aceste liste implică activități de prelucrare care presupun furnizarea de bunuri sau prestarea de servicii către persoane vizate sau monitorizarea comportamentului acestora în mai multe state membre ori care pot afecta în mod substanțial libera circulație a datelor cu caracter personal în cadrul Uniunii.[91]

Evaluarea conține cel puțin:

(a) o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;

(b) o evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri;

(c) o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate menționate la alineatul (1); și

(d) măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentului regulament, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor persoane interesate.

La evaluarea impactului operațiunilor de prelucrare efectuate de operatorii sau de persoanele împuternicite de operatori relevante, se are în vedere în mod corespunzător respectarea de către operatorii sau persoanele împuternicite respective a codurilor de conduită aprobate, în special în vederea unei evaluări a impactului asupra protecției datelor.

---

[90] Adunarea Generală a ONU, Proiect de rezoluție revizuită privind dreptul la viață privată în era digitală, A/C.3/71/L.39/Rev. 1, New York, 16 noiembrie 2016; ONU, Consiliul pentru Drepturile Omului, Dreptul la viață privată în era digitală, A/HRC/34/L.7/Rev. 1, 22 martie 2017.

[91] Hotărârea CJUE din 24 noiembrie 2011 în cauzele conexate C-468/10 și C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) și Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado, punctul 29.

Operatorul solicită, acolo unde este cazul, avizul persoanelor vizate sau al reprezentanților acestora privind prelucrarea prevăzută, fără a aduce atingere protecției intereselor comerciale sau publice ori securității operațiunilor de prelucrare.

Atunci când prelucrarea are un temei juridic în dreptul Uniunii sau al unui stat membru sub incidența căruia intră operatorul, iar dreptul respectiv reglementează operațiunea de prelucrare specifică sau setul de operațiuni specifice în cauză și deja s-a efectuat o evaluare a impactului asupra protecției datelor ca parte a unei evaluări a impactului generale în contextul adoptării respectivului temei juridic, alineatele (1)-(7)din art.6 al Regulamentului, nu se aplică, cu excepția cazului în care statele membre consideră că este necesară efectuarea unei astfel de evaluări înaintea desfășurării activităților de prelucrare.

Acolo unde este necesar, operatorul efectuează o analiză pentru a evalua dacă prelucrarea are loc în conformitate cu evaluarea impactului asupra protecției datelor, cel puțin atunci când are loc o modificare a riscului reprezentat de operațiunile de prelucrare.

Responsabilul cu protecția datelor este desemnat pe baza calităților profesionale și, în special, a cunoștințelor de specialitate în dreptul și practicile din domeniul protecției datelor, precum și pe baza capacității de a îndeplini sarcinile prevăzute la articolul 39 din Regulament.

Responsabilul cu protecția datelor poate fi un membru al personalului operatorului sau persoanei împuternicite de operator sau poate să își îndeplinească sarcinile în baza unui contract de servicii.

Operatorul sau persoana împuternicită de operator publică datele de contact ale responsabilului cu protecția datelor și le comunică autorității de supraveghere.

Riscul pentru drepturile și libertățile persoanelor fizice, prezentând grade diferite de probabilitate de materializare și de gravitate, poate fi rezultatul unei prelucrări a datelor cu caracter personal care ar putea genera prejudicii de natură fizică, materială sau morală, în special în cazurile în care:

- ✓ prelucrarea poate conduce la discriminare, furt sau fraudă a identității, pierdere financiară, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional, inversarea neautorizată a pseudonimizării sau la orice alt dezavantaj semnificativ de natură economică sau socială;
- ✓ persoanele vizate ar putea fi private de drepturile și libertățile lor sau împiedicate să-și exercite controlul asupra datelor lor cu caracter personal;
- ✓ datele cu caracter personal prelucrate sunt date care dezvăluie originea rasială sau etnică, opiniile politice, religia sau convingerile filozofice, apartenența sindicală; sunt prelucrate date genetice, date privind sănătatea sau date privind viața sexuală sau privind condamnările penale și infracțiunile sau măsurile de securitate conexe;
- ✓ sunt evaluate aspecte de natură personală, în special analizarea sau previzionarea unor aspecte privind randamentul la locul de muncă, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările, în scopul de a se crea sau de a se utiliza profiluri personale;
- ✓ sunt prelucrate date cu caracter personal ale unor persoane vulnerabile, în special ale unor copii; sau prelucrarea implică un volum mare de date cu caracter personal și afectează un număr larg de persoane vizate.[92]

[92]Irina Alexe, Daniel-Mihail Șandru (editori), Legislația privind protecția datelor în România, Ed. Rosetti Internațional, București, 2018, ISBN 978-6068794-90-7, pag.216

Pentru a favoriza respectarea dispozițiilor prezentului regulament în cazurile în care operațiunile de prelucrare sunt susceptibile să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul ar trebui să fie responsabil de efectuarea unei evaluări a impactului asupra protecției datelor, care să estimeze, în special, originea, natura, specificitatea și gravitatea acestui risc.

Rezultatul evaluării ar trebui luat în considerare la stabilirea măsurilor adecvate care trebuie luate pentru a demonstra că prelucrarea datelor cu caracter personal respectă prezentul regulament. În cazul în care o evaluare a impactului asupra protecției datelor arată că operațiunile de prelucrare implică un risc ridicat, pe care operatorul nu îl poate atenua prin măsuri adecvate sub aspectul tehnologiei disponibile și al costurilor implementării, ar trebui să aibă loc o consultare a autorității de supraveghere înainte de prelucrare.

În cazul în care o evaluare a impactului asupra protecției datelor arată că prelucrarea ar genera, în absența garanțiilor, măsurilor de securitate și mecanismelor de atenuare a riscului, un risc ridicat pentru drepturile și libertățile persoanelor fizice, iar operatorul consideră că riscul nu poate fi atenuat prin mijloace rezonabile sub aspectul tehnologiilor disponibile și al costurilor implementării, autoritatea de supraveghere ar trebui să fie consultată înainte de începerea activităților de prelucrare.

Un astfel de risc ridicat este susceptibil să fie generat de anumite tipuri de prelucrare, precum și de amploarea și frecvența prelucrării, care pot duce și la producerea unor prejudicii sau pot atinge drepturile și libertățile persoanelor fizice. Autoritatea de supraveghere ar trebui să răspundă cererii de consultare într-un anumit termen.

Cu toate acestea, lipsa unei reacții din partea autorității de supraveghere în termenul respectiv ar trebui să nu aducă atingere niciunei intervenții a autorității de supraveghere în conformitate cu sarcinile și competențele sale prevăzute în prezentul regulament, inclusiv competența de a interzice operațiuni de prelucrare. Ca parte a acestui proces de consultare, rezultatul unei evaluări a impactului asupra protecției datelor efectuate cu privire la prelucrarea în cauză poate fi transmis autorității de supraveghere, în special măsurile avute în vedere pentru a atenua riscul pentru drepturile și libertățile persoanelor fizice.[93]

În cazul în care prelucrarea datelor cu caracter personal se desfășoară în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator din Uniune, iar operatorul sau persoana împuternicită de operator are sedii în mai multe state membre, sau în cazul în care prelucrarea care se desfășoară în contextul activităților unui singur sediu al unui operator sau al unei persoane împuternicite de operator din Uniune afectează sau este susceptibilă să afecteze semnificativ persoane vizate din mai multe state membre, autoritatea de supraveghere a sediului principal al operatorului sau al persoanei împuternicite de operator ori a sediului unic al operatorului sau al persoanei împuternicite de operator ar trebui să acționeze în calitate de autoritate principală.

Aceasta ar trebui să coopereze cu celelalte autorități vizate, pentru că operatorul sau persoana împuternicită de operator are un sediu pe teritoriul statului lor membru, pentru că persoanele vizate care își au reședința pe teritoriul lor sunt afectate în mod semnificativ sau pentru că le-a fost înaintată o plângere. De asemenea, în cazul în care

[93]Irina Alexe, Reforma instituțională, în materia protecției datelor, la nivel european, în volumul Regulamentul general privind protecția datelor. Comentarii și explicații, coordonator Andrei Săvescu, Editura Hamangiu, 2018, p.11

o persoană vizată care nu își are reședința în statul membru respectiv a depus o plângere, autoritatea de supraveghere la care a fost depusă plângerea ar trebui, de asemenea, să fie o autoritate de supraveghere vizată.

În cadrul sarcinilor sale de a emite orientări cu privire la orice chestiune referitoare la punerea în aplicare a prezentului regulament, comitetul ar trebui să poată emite orientări privind, în special, criteriile care trebuie luate în considerare pentru a se stabili dacă prelucrarea în cauză afectează în mod semnificativ persoane vizate din mai multe state membre și privind conținutul unei obiecții relevante și motivate.

Fiecare autoritate de supraveghere care nu acționează ca autoritate de supraveghere principală ar trebui să aibă competența de a trata cazuri locale, în care operatorul sau persoana împuternicită de operator are sedii în mai multe state membre, dar obiectul respectivei prelucrări privește doar prelucrarea efectuată într-un singur stat membru și implicând doar persoane vizate din acel unic stat membru, de exemplu în cazul în care obiectul îl constituie prelucrarea datelor cu caracter personal ale angajaților în contextul specific legat de forța de muncă dintr-un stat membru.

În astfel de cazuri, autoritatea de supraveghere ar trebui să informeze fără întârziere autoritatea de supraveghere principală cu privire la această chestiune. După ce a fost informată, autoritatea de supraveghere principală ar trebui să decidă dacă va trata ea însăși cazul în temeiul dispoziției privind cooperarea între autoritatea de supraveghere principală și alte autorități de supraveghere vizate ("mecanismul ghișeului unic"), sau dacă autoritatea de supraveghere care a informat-o ar trebui să se ocupe de caz la nivel local.[94]

Atunci când decide dacă va trata cazul, autoritatea de supraveghere principală ar trebui să ia în considerare dacă există un sediu al operatorului sau al persoanei împuternicite de operator în statul membru al autorității de supraveghere care a informat-o, în vederea garantării respectării efective a unei decizii în ceea ce privește operatorul sau persoana împuternicită de operator. În cazul în care autoritatea de supraveghere principală decide să trateze cazul, autoritatea de supraveghere care a informat-o ar trebui să beneficieze de posibilitatea de a prezenta un proiect de decizie, de care autoritatea de supraveghere principală ar trebui să țină seama în cea mai mare măsură atunci când pregătește proiectul său de decizie în cadrul respectivului mecanism al ghișeului unic.

În cazurile în care o altă autoritate de supraveghere ar trebui să acționeze în calitate de autoritate de supraveghere principală pentru activitățile de prelucrare ale operatorului sau ale persoanei împuternicite de operator, dar obiectul concret al unei plângeri sau posibila încălcare vizează numai activitățile de prelucrare ale operatorului sau ale persoanei împuternicite de operator în statul membru în care a fost depusă plângerea sau a fost depistată posibila încălcare, iar chestiunea nu afectează în mod substanțial sau nu este susceptibilă să afecteze în mod substanțial persoane vizate din alte state membre, autoritatea de supraveghere care a primit o plângere sau a depistat ori a fost informată în alt mod asupra unor situații de posibile încălcări ale prezentului regulament ar trebui să încerce o soluționare pe cale amiabilă cu operatorul și, în cazul în care aceasta eșuează, să își exercite plenitudinea competențelor.

[94]Consiliul Europei (2013), jurisprudențaCurții Europene a Drepturilor Omului în ceea ce privețteprotecția datelor cu caracter personal, Jurisprudența DP (2013), disponibilă la: www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP%202013%20Case%20Law_Eng%20%28final%2018%2007%202013%29.pdf

Aceasta ar trebui să includă activități specifice de prelucrare efectuate pe teritoriul statului membru al autorității de supraveghere ori cu privire la persoane vizate de pe teritoriul acelui stat membru, activități de prelucrare care au loc în contextul unei oferte de bunuri sau servicii destinate în mod special persoanelor vizate pe teritoriul statului membru al autorității de supraveghere sau activități de prelucrare care trebuie evaluate ținând seama de obligațiile juridice relevante în temeiul dreptului intern.

Funcția responsabilului cu protecția datelor

Operatorul și persoana împuternicită de operator se asigură că responsabilul cu protecția datelor este implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal.

Operatorul și persoana împuternicită de operator sprijină responsabilul cu protecția datelor în îndeplinirea sarcinilor menționate la articolul 39, asigurându-i resursele necesare pentru executarea acestor sarcini, precum și accesarea datelor cu caracter personal și a operațiunilor de prelucrare, și pentru menținerea cunoștințelor sale de specialitate.

Operatorul și persoana împuternicită de operator se asigură că responsabilul cu protecția datelor nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea acestor sarcini. Acesta nu este demis sau sancționat de către operator sau de persoana împuternicită de operator pentru îndeplinirea sarcinilor sale. Responsabilul cu protecția datelor răspunde direct în fața celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator.

Persoanele vizate pot contacta responsabilul cu protecția datelor cu privire la toate chestiunile legate de prelucrarea datelor lor și la exercitarea drepturilor lor în temeiul prezentului regulament.[95]

Responsabilul cu protecția datelor are obligația de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale, în conformitate cu dreptul Uniunii sau cu dreptul intern.

Responsabilul cu protecția datelor poate îndeplini și alte sarcini și atribuții. Operatorul sau persoana împuternicită de operator se asigură că niciuna dintre aceste sarcini și atribuții nu generează un conflict de interese.

Sarcinile responsabilului cu protecția datelor

Responsabilul cu protecția datelor are cel puțin următoarele sarcini:

- ✓ informarea și consilierea operatorului, sau a persoanei împuternicite de operator, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care

[95] Autoritatea Europeana pentru Protecția Datelor (AEPD) (2011), Public access to documents containing personal data after the Bavarian Lager ruling (Accesul public la documente care conțin date cu caracter personal în urma hotărârii din cauza BavarianLager), Bruxelles, 24 martie 2011, disponibile la: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf

le revin în temeiul prezentului regulament și al altor dispoziții de drept al Uniunii sau drept intern referitoare la protecția datelor;

- ✓ monitorizarea respectării prezentului regulament, a altor dispoziții de drept al Uniunii sau de drept intern referitoare la protecția datelor și a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;
- ✓ furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia, în conformitate cu articolul 35;
- ✓ cooperarea cu autoritatea de supraveghere;
- ✓ asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menționată la articolul 36, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.

În îndeplinirea sarcinilor sale, responsabilul cu protecția datelor ține seama în mod corespunzător de riscul asociat operațiunilor de prelucrare, luând în considerare natura, domeniul de aplicare, contextul și scopurile prelucrării.[96]

[96]FRA (2010), Drepturi fundamentale: provocări și realizări în 2010, Raport anual 2010, p. 59. FRA a abordat acest aspect în detaliu în raportul privind Protecția datelor în Uniunea Europeană: rolul autorităților naționale pentru protecția datelor, publicat în mai 2010, disponibil pe https://fra.europa.eu/sites/default/files/fra_2011_01980000_ro_tra_dr2.pdf

CAP. V ASPECTE SPECIFICE CU PRIVIRE LA ROLUL SI ACTIVITATEA RESPONSABILULUI PENTRU PROTECȚIA DATELOR CU CARACTER PERSONAL

Noțiunea de responsabil cu protecția datelor cu caracter personal

- Responsabilul cu protecţia datelor cu caracter personal (DPO), este aceea persoană care este desemnată pe baza calităţilor profesionale şi, în special, a cunoştinţelor de specialitate în dreptul şi practicile din domeniul protecţiei datelor, precum şi pe baza capacităţii de a îndeplini sarcinile prevăzute la articolul 39.

Desemnarea responsabilului cu protecția datelor cu caracter personal

(1) Operatorul şi persoana împuternicită de operator desemnează un responsabil cu protecţia datelor ori de câte ori:

a)prelucrarea este efectuată de o autoritate sau un organism public, cu excepţia instanţelor care acţionează în exerciţiul funcţiei lor jurisdicţionale;

b)activităţile principale ale operatorului sau ale persoanei împuternicite de operator constau în operaţiuni de prelucrare care, prin natura, domeniul de aplicare şi/sau scopurile lor, necesită o monitorizare periodică şi sistematică a persoanelor vizate pe scară largă;

c)activităţile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date, menţionată la articolul 9, sau a unor date cu caracter personal privind condamnăripenaleşi infracţiuni, menţionată la articolul 10.

(2) Un grup de organizații poate numi un responsabil cu protecţia datelor unic, cu condiţia ca responsabilul cu protecţia datelor să fie uşor accesibil din fiecare întreprindere.

(3)În cazul în care operatorul sau persoana împuternicită de operator este o autoritate publică sau un organism public, poate fi desemnat un responsabil cu protecţia datelor unic pentru mai multe dintre aceste autorităţi sau organisme, luând în considerare structura organizatorică şi dimensiunea acestora.

(4)În alte cazuri decât cele menţionate la alineatul (1), operatorul sau persoana împuternicită de operator ori asociaţiile şi alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori pot desemna sau, acolo unde dreptul Uniunii sau dreptul intern solicită acest lucru, desemnează un

responsabil cu protecţia datelor. Responsabilul cu protecţia datelor poate să acţioneze în favoarea unor astfel de asociaţii şi alte organisme care reprezintă operatori sau persoane împuternicite de operatori.

(5) Responsabilul cu protecţia datelor este desemnat (pe baza calităţilor profesionale şi, în special, a cunoştinţelor de specialitate în dreptul şi practicile din domeniul protecţiei datelor, precum şi pe baza capacităţii de a îndeplini sarcinile prevăzute la articolul 39. (Conform art. 37 alin. (5) extras din GDPR)

(6) Responsabilul cu protecţia datelor poate fi un membru al personalului operatorului sau persoanei împuternicite de operator sau poate să îşi îndeplinească sarcinile în baza unui contract de servicii.

(7) Operatorul sau persoana împuternicită de operator publică datele de contact ale responsabilului cu protecţia datelor şi le comunică autorităţii de supraveghere.

Calitățile profesionale pe care trebuie să le posede un DPO

- DPO trebuie desemnat pe baza calităților profesionale și, în special a cunoștințelor de specialitate în dreptul și practicile în domeniul protecției datelor, precum șipe baza capacității de a-și îndeplini sarcinile.
- Nivelul de expertiză necesar ar trebui determinat pe baza operațiunilor de prelucrare efectuate și a protecției necesare pentru datele cu caracter personal prelucrate. De exemplu, în situația în care o operațiune de prelucrare a datelor este deosebit de complexă sau în cazul în care este implicat un volum mare de date speciale, DPO poate necesita un nivel mai ridicat de expertiză și suport.

Calitățile profesionale pe care trebuie să le posede un DPO
(Conform Art. 37(6) din GDPR)

Aptitudinile și expertiza relevante includ:

- ✓ experiență în legislația și practicile de protecție a datelor la nivel național și european, precum și o înțelegere complexă a RGPD
- ✓ înțelegerea operațiunilor de prelucrare efectuate
- ✓ înțelegerea tehnologiilor de informații și de securitate a datelor
- ✓ cunoașterea sectorului de afaceri și a organizației
- ✓ abilitatea de a promova protecția datelor în cadrul organizației

Rolul și atribuțiile responsabilului cu protecția datelor cu caracter personal.

- Responsabilul cu protecția datelor (DPO) are un rol important conform prevederilor GDPR și reprezintă un pas necesar în procesul de conformare al organizației la noile reglementări.

- Această persoană trebuie să poate să monitorizeze și să evalueze procesarea datelor în cadrul organizației.

(1) Responsabilul cu protecţia datelor are cel puţin următoarele sarcini:

a)informarea şi consilierea operatorului, sau a persoanei împuternicite de operator, precum şi a angajaţilor care se ocupă de prelucrare cu privire la obligaţiile care le revin în temeiul prezentului regulament şi al altor dispoziţii de drept al Uniunii sau drept intern referitoare la protecţia datelor;

b)monitorizarea respectării prezentului regulament, a altor dispoziţii de drept al Uniunii sau de drept intern referitoare la protecţia datelor şi a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce priveşte protecţia datelor cu caracter personal, inclusiv alocarea responsabilităţilor şi acţiunile de sensibilizare şi de formare a personalului implicat în operaţiunile de prelucrare, precum şi auditurile aferente;

c)furnizarea de consiliere la cerere în ceea ce priveşte evaluarea impactului asupra protecţiei datelor şi monitorizareafuncţionării acesteia, în conformitate cu articolul 35;

d)cooperarea cu autoritatea de supraveghere;

e)asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menţionată la articolul 36, precum şi, dacă este cazul, consultarea cu privire la orice altă chestiune.

(2)În îndeplinirea sarcinilor sale, responsabilul cu protecţia datelor ţine seama în mod corespunzător de riscul asociat operaţiunilor de prelucrare, luând în considerare:

- natura,
- domeniul de aplicare,
- contextual
- scopurile prelucrării.

Funcţia responsabilului cu protecţia datelor

(1) Operatorul şi persoana împuternicită de operator se asigură că responsabilul cu protecţia datelor este implicat în mod corespunzător şi în timp util în toate aspectele legate de protecţia datelor cu caracter personal.

(2) Operatorul şi persoana împuternicită de operator sprijină responsabilul cu protecţia datelor în îndeplinirea sarcinilor menţionate la articolul 39, asigurându-i resursele necesare pentru executarea acestor sarcini, precum şi accesarea datelor cu caracter personal şi a operaţiunilor de prelucrare, şi pentru menţinerea cunoştinţelor sale de specialitate.

(3) Operatorul şi persoana împuternicită de operator se asigură că responsabilul cu protecţia datelor nu primeşte niciun fel de instrucţiuni în ceea ce priveşte îndeplinirea acestor sarcini. Acesta nu este demis sau sancţionat de către operator sau de persoana împuternicită de operator pentru îndeplinirea sarcinilor sale.

(4)Persoanele vizate pot contacta responsabilul cu protecţia datelor cu privire la toate chestiunile legate de prelucrarea datelor lor şi la exercitarea drepturilor lor în temeiul prezentului regulament.

(5)Responsabilul cu protecţia datelor are obligaţia de a respecta secretul sau confidenţialitatea în ceea ce priveşte îndeplinirea sarcinilor sale, în conformitate cu dreptul Uniunii sau cu dreptul intern.

(6)Responsabilul cu protecţia datelor poate îndeplini şi alte sarcini şi atribuţii. Operatorul sau persoana împuternicită de operator se asigură că niciuna dintre aceste sarcini şi atribuţii nu generează un conflict de interese.

Rolul responsabilului cu protecţia datelor:

- ✓ **să informeze și să consilieze** operatorul sau persoana împuternicită de operator, precum și angajații acestora cu privire la obligațiile existente în domeniul protecției datelor cu caracter personal;
- ✓ **să monitorizeze respectarea GDPR** și a legislației naționale în domeniul protecției datelor;
- ✓ **să consilieze operatorul sau persoana împuternicită** în legătură cu realizarea de studii de impact privind protecţia datelor și să verifice efectuarea acestora;
- ✓ **să coopereze cu autoritatea pentru protecţia datelor** și să reprezinte punctul de contact în relaţia cu aceasta.

Rolul DPO în evaluarea impactului operațiunilor de prelucrare:

- ➢ **Operatorul** și **nu DPO** efectuează, atunci când este necesar, o **evaluare a impactului operațiunilor de prelucrare** („DPIA”).
- ➢ Cu toate acestea, DPO are un rol foarte important și util în **asistarea operatorului**.
- ➢ Potrivit principiului protecția datelor începând cu momentul conceperii, operatorul „solicita avizul” DPO la realizarea DPIA.
- ➢ DPO „ofera consiliere la cerere în ceea ce privește DPIA și monitorizeaza funcționarea acesteia, în conformitate cu RGPD”.

Sarcinile Responsabilului cu protecția datelor (DPO):

1. **Informarea organizației și persoanelor vizate** cu privire la drepturile și obligatiile lor în baza legislației privind protecția datelor cu caracter personal.
2. **Monitorizarea implementării legislației** privind protecția datelor cu caracter personal și standardele specifice la care organizația a aderat.

3. Recomandări și asistență de specialitate organizației cu privire la interpretarea și aplicarea prevederilor legislației privind protecția datelor cu caracter personal.
4. **Gestionarea relației cu ANSPDCP – Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal.**
5. **Respectarea principiului obiectivității** în domeniul protecția datelor cu caracter personal.
6. **Asigurarea și gestionarearegistrului de evidență al prelucrării datelor cu caracter personal.**
7. **Gestionarea și coordonarea resurselor umane, financiare, tehnice necesare realizări sarcinilor și activităților specifice domeniului protecției datelor cu caracter personal.**
8. **Dezvoltarea profesională continuă în domeniul protecției datelor cu caracter personal atât a sa cât si a angajaților din companie care sunt direct implicați în prelucrarea datelor cu caracter personal.**
9. **Monitorizarea aplicarii** instrumentelor și metodelor de îmbunătățire a eficacitatii sistemului de management al securitatii informatiei.
10. **Analiza si evaluarea riscurilor** de prelucrare a datelor cu caracter personal.

Ca parte a acestor sarcini de monitorizare a conformității, **DPO** poate, în special:

- să colecteze informații pentru identificarea operațiunilor de prelucrare.
- să analizeze și să verifice conformitatea operațiunilor de prelucrare
- să informeze, să consilieze și să emită recomandări operatorului sau persoanei împuternicite de operator.

Responsabilul cu protecția datelor trebuie să aibă calitățile profesionale și cunoștințele profesionale adecvate recunoscute de legislația privind protecția datelor.

În prezent, nu există o cerință expresă de a deține o anumită calificare sau certificare. Cu toate acestea, deținerea unei certificări în conformitate cu GDPR este o modalitate eficientă de a **demonstra** cunoștințele experților.

Conform GDPR, ca DPO acesta trebuie să beneficieze de toate condițiile și tot suportul organizației pentru a avea acces la cele mai performante resurse de instruire.

Un **DPO trebuie să fie independent**.

- Acest lucru nu înseamnă neapărat că, în calitate de operator sau procesator, trebuie să numiți o persoană externă; rolul DPO poate fi îndeplinit de un angajat.
- Postul poate fi un rol cu jumătate de normă sau combinat cu alte sarcini, însă, în îndeplinirea rolului, DPO trebuie să aibă o linie independentă de raportare și să fie împuternicit să raporteze direct comitetului fără intervenție.

Cine nu poate fi DPO în organizație?

- Art. 38(6) permite DPO "să îndeplinească și alte sarcini și atribuții". Cu toate acestea, este nevoie ca organizațiasă se asigure că "niciuna dintre aceste sarcini și atribuții nu generează un conflict de interese".
- Absența conflictului de interese este strâns legată de obligația de a acționa în mod independent.
- Cu toate că îi este permis să aibă și alte funcții, acestuia îi pot fi încredințate alte sarcini și atribuții cu condiția ca acestea să nu dea naștere unor conflicte de interese. Acest lucru presupune, în special, faptul că DPO nu poate deține o poziție în cadrul organizației care ar conduce la posibilitatea ca DPO să stabilească scopurile și mijloacele de prelucrare a datelor cu caracter personal.
- Acest lucru trebuie luat în considerare de la caz la caz, ținând-se cont de structura organizațională specifică fiecărei organizații.

GDPR penalizează grav conflictul de interese

Funcții din cadrul organizației cu care DPO poate intra în conflict de interese pot include funcțiide conducere cum ar fi: administratorul / managerul companiei, director executiv, director operațional, director financiar, șeful serviciului medical, șeful departamentului de marketing, șeful departamentului de resurse umane, șeful departamentului IT, sau alte funcții inferioare dacă acestea conduc la posibilitatea de a stabili scopurile și mijloacelor de prelucrare.

Monitorizarea conformității NU înseamnă că DPO (responsabilul) este personal responsabil în situația în care există un caz de nerespectarea prevederilor GDPR.

GDPR precizează:

- **Operatorul**, și nu DPO, are obligația de a „pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul Regulament”.
- **Respectarea normelor de protecției a datelor este o responsabilitate corporativă a operatorului și nu a DPO**.

Operatorul solicită avizul DPO în legătură cu următoarele aspecte, printre care:

- dacă să efectueze sau nu DPIA;
- ce metodologie să fie folosită la efectuarea DPIA;
- dacă să efectueze DPIA intern sau să externalizeze;

- ce garanții (inclusiv măsuri tehnice și organizaționale) să pună în aplicare pentru reducerea oricăror riscuri la adresa drepturilor și intereselor persoanelor vizate;
- dacă DPIA a fost sau nu efectuată corect și dacă respectivele concluzii (dacă să continue sau nu prelucrarea și ce garanții să pună în aplicare) respectă GDPR.

Atenție !!!

- ***Responsabilul pentru protecția datelor nu poate fi demis sau sancționat de operator sau persoana împuternicită de operator pentru îndeplinirea sarcinilor sale. De exemplu, responsabilul nu poate fi demis pentru oferirea unui sfat conform sacinilor sale.***
- *Un responsabil cu protecția datelor ar putea fi totuși demis, în mod legal, din alte motive decât cele privind îndeplinirea sarcinilor sale în această calitate. De exemplu, responsabilul poate fi demis în caz de furt, hărțuire ori o abatere gravă similară.*

Poziția responsabilului cu protecția datelor cu caracter personal în cadrul organizației

- Responsabilul cu protecția datelor cu caracter personal trebuie să poată să își desfășoare activitatea independent de ierarhie. În acest sens este necesară o poziționare optimă în cadrul organigramei organizaționale.
- Este necesar să aibă acces la toate operațiunile de prelucare a datelor, până la cel mai înalt nivel al conducerii.

Principiul obiectivității în desfășurarea sarcinilor și activităților responsabilului cu protecția datelor cu caracter personal

Principiul obiectivității impune o obligație tuturor DPO de a nu își compromite profesia din cauza unor erori, conflicte de interese sau din cauza influenței nedorite a unor alte persoane.

Resursele necesare responsabilului cu protecția datelor cu caracter personal în vedere îndeplinirii atribuțiilor sale:

DPO trebuie să beneficieze de resursele necesare pentru îndeplinirea sarcinilor sale.

În funcție de natura operațiunilor de prelucrare și a activităților și dimensiunii organizației, trebuie asigurate următoarele resurse pentru DPO:

- sprijin activ al funcției DPO din partea managementului superior;
- timp suficient pentru DPO în vederea îndeplinirii atribuțiilor sale;
- sprijin corespunzător în ceea ce privește resursele financiare, infrastructură (sediu, facilități, echipament) și personal, după caz;

- comunicare oficială către angajați cu privire la desemnarea DPO;
- accesul necesar la alte servicii precum resurse umane, juridic,IT, securitate etc. astfel încât DPO să beneficieze de un sprijin esențial, reacții și informații din partea altor servicii;
- pregătire continuă.

Obligațiile responsabilului cu protecția datelor cu caracter personal din perspectiva dezvoltării profesionale continue. Metode de responsabilizare a personalului organizației.

- Responsabilului cu protecția datelor cu caracter personal, trebuie să fie suficient de pregătit și de calificat încât să își poată îndeplini rolul.
- Trebuie să înțeleagă atât prevederile regulamentului cât și aspectele tehnice ca să aiba o imagine corectă asupra manierei în care datele sunt colectate, procesate și stocate.
- Trebuie să aiba în vedere activitatea de perfecționare continuă în ceea ce privește legislația și cerințele legate de prelucrarea și protecția datelor cu caracter personal.

Răspunderea responsabilului cu protecția datelor cu caracter personal

- În cazul în care va avea loc o prelucrare cu risc ridicat (cum ar fi monitorizarea activități, evaluări sistematice sau procesări speciale ale unor categorii de date), trebuie să fie efectuată o evaluare detaliată a impactului asupra vieții private („PIA").
- În cazul în care o evaluare "PIA" are ca rezultat concluzia că există într-adevăr un nivel de risc ridicat pentru persoanele vizate, controlorii/responsabilul trebuie să notifice supraveghetorul și să obțină punctul de vedere asupra caracterului adecvat al măsurilor propuse de evaluarea PIA pentru a reduce riscurile de prelucrare.

CAP. VI METODOLOGII DE EVALUARE A IMPACTULUI ASUPRA PROTECȚIEI DATELOR (DPIA) ȘI STABILIREA DACĂ O PRELUCRARE ESTE

"SUSCEPTIBILĂ SĂ GENEREZE UN RISC RIDICAT"

Evaluarea impactului asupra protecției datelor (DPIA) este prevăzută în Art. 35 din Regulamentul 2016/679 (GDPR/RGPD).

Analiza DPIA este un instrument care este conceput pentru evaluarea respectării obligațiilor de protecție a datelor de către operatorii de prelucrare a datelor cu caracter personal (entități publice și private) și pentru a identifica eventualele riscuri și strategii de reducere a lor. Acest instrument transpus în practică poate demonstra că operatorul care realizează prelucrări de date cu caracter personal, a luat masurile adecvate pentru a respecta cerințeleGDPR.

DPIA este un proces destinat să descrie prelucrarea, să evalueze necesitatea și proporționalitatea acesteia și să contribuie la gestionarea riscurilor la adresa drepturilor și libertăților persoanelor vizate rezultate din prelucrarea datelor cu caracter personal, prin evaluarea acestora și stabilirea de măsuri pentru atenuarea lor.

O evaluare DPIA ar trebui, în mod ideal, să fie realizată încă din faza de proiectare a unui nou tip de prelucrare, sistem sau program care prelucrează date cu caracter personal și apoi revizuită atunci când cerințele privind programul și obligațiile legale suferă schimbări. Rezumând cele enunțate se desprinde concluzia că Evaluarea Impactului asupra protecției datelor (DPIA), reprezintă un proces pentru construirea și demonstrarea conformității cu GDPR.

GDPR nu definește în mod formal conceptul de DPIA ca atare, dar specifică conținutul său minim (conform art. 35 (7)).

Pentru a respectarea cerințele GDPR privind protecția datelor, în cazul în care operațiunile de prelucrare pot duce la un risc ridicat pentru drepturile și libertățile persoanelor fizice(art. 35 (1)), operatorul trebuie să realizeze DPIA (art. 35 (3)) pentru a evalua, în special, originea, natura, particularitatea și gravitatea acestui risc.

Este necesară o DPIA cel puțin în următoarele cazuri:

- evaluare sistematică și cuprinzătoare a aspectelor personale referitoare la o persoană fizică, inclusiv crearea de profiluri;
- prelucrarea pe scară largă a unor date sensibile;
- monitorizarea sistematică pe scară largă a unor zone accesibile publicului.

O listă cu 7 situații în care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal a fost a întocmita și publicata de Autoritatea națională de supraveghere prin Decizia nr. 174 din 2018. Aceasta listă nu este însă exhaustivă. Evaluarea impactului asupra protecției datelor este necesară și în cazul în care o prelucrare de date, deși nu se regăsește în acea lista, este susceptibilă de a genera un risc ridicat pentru drepturile și libertățile persoanelor fizice.

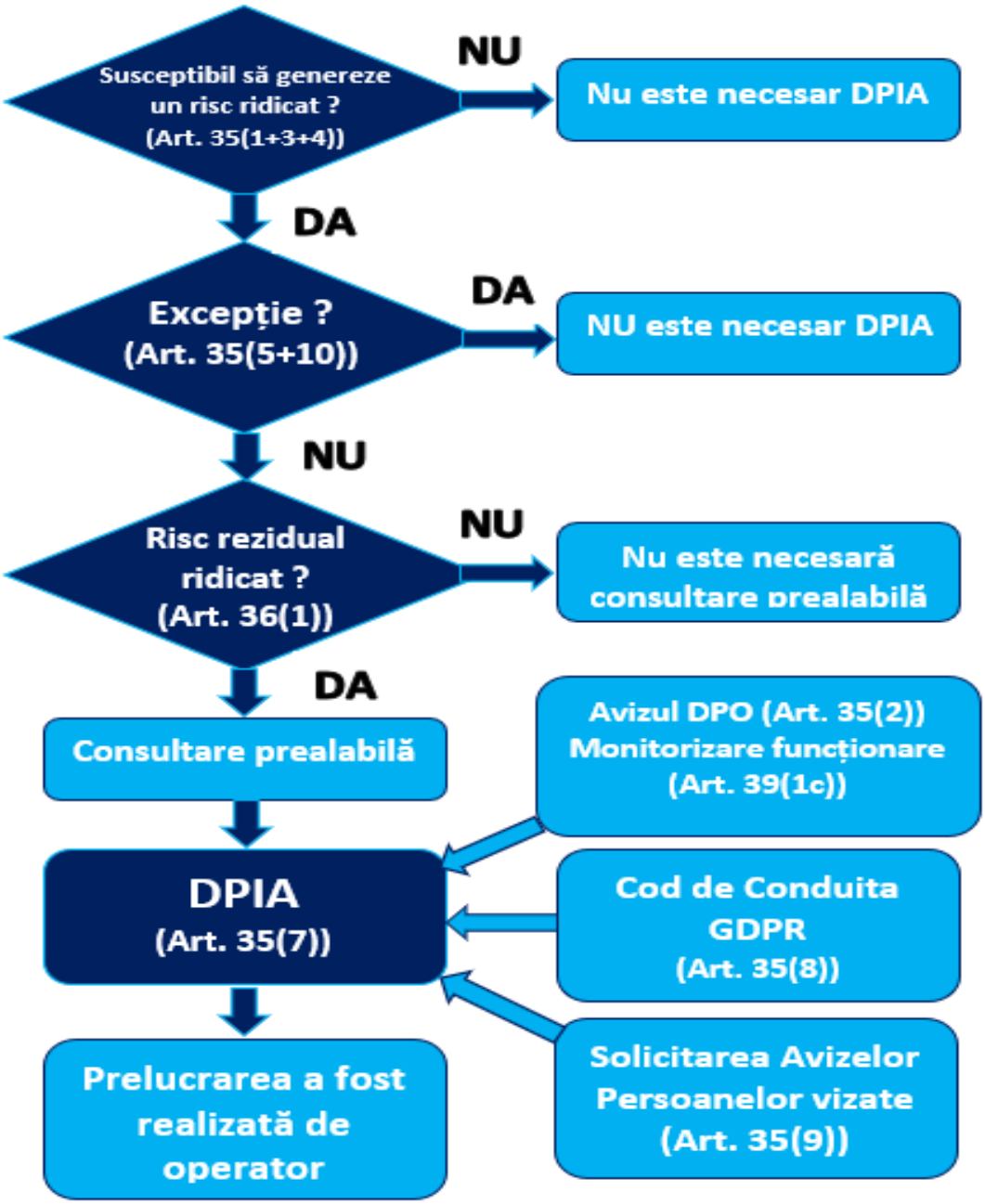
Decizia ANSPDCP privind lista operațiunilor pentru care este obligatorie realizarea DPIA

În Monitorul Oficial al României, partea I, nr. 919 din data de 31 octombrie 2018, a fost publicată Decizia nr. 174/2018 privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal.

Evaluarea impactului asupra protecţiei datelor cu caracter personal de către operatori este obligatorie în special în următoarele cazuri:

1. prelucrarea datelor cu caracter personal în vederea realizării unei evaluări sistematice şi cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, şi care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;
2. prelucrarea pe scară largă a datelor cu caracter personal privind originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenenţa la sindicate, a datelor genetice, a datelor biometrice pentru identificarea unică a unei persoane fizice, a datelor privind sănătatea, viaţa sexuală sau orientarea sexuală ale unei persoane fizice sau a datelor cu caracter personal referitoare la condamnări penale şi infracţiuni;
3. prelucrarea datelor cu caracter personal având ca scop monitorizarea sistematică pe scară largă a unei zone accesibile publicului, cum ar fi supravegherea video în centre comerciale, stadioane, pieţe, parcuri sau alte asemenea spaţii;
4. prelucrarea pe scară largă a datelor cu caracter personal ale persoanelor vulnerabile, în special ale minorilor şi ale angajaţilor, prin mijloace automate de monitorizare şi/sau înregistrare sistematică a comportamentului, inclusiv în vederea desfăşurării activităţilor de reclamă, marketing şi publicitate;
5. prelucrarea pe scară largă a datelor cu caracter personal prin utilizarea inovatoare sau implementarea unor tehnologii noi, în special în cazul în care operaţiunile respective limitează capacitatea persoanelor vizate de a-şi exercita drepturile, cum ar fi utilizarea tehnicilor de recunoaştere facială în vederea facilitării accesului în diferite spaţii;
6. prelucrarea pe scară largă a datelor generate de dispozitive cu senzori care transmit date prin internet sau prin alte mijloace (aplicaţii "Internetul lucrurilor", cum ar fi smart TV, vehicule conectate, contoare inteligente, jucării inteligente, oraşe inteligente sau alte asemenea aplicaţii);
7. prelucrarea pe scară largă şi/sau sistematică a datelor de trafic şi/sau de localizare a persoanelor fizice (cum ar fi monitorizarea prin Wi-Fi, prelucrarea datelor de localizare geografică a pasagerilor în transportul public sau alte asemenea situaţii) atunci când prelucrarea nu este necesară pentru prestarea unui serviciu solicitat de persoana vizată.

Principiile de bază legate de DPIA conform GDPR



Componenta unei DPIA

Potrivit art. 35 (7) și a Considerentelor 84 și 90), DPIA trebuie să includă:

- descrierea operațiunilor de prelucrare preconizate și scopurilor prelucrării;
- evaluarea necesității și proporționalității prelucrării;
- evaluarea riscurilor pentru drepturile și libertățile persoanelor vizate;

- măsurile preconizate în vederea:
  - abordării riscurilor;
  - demonstrării conformității cu dispozițiile GDPR.

Obligativitatea realizarării unei DPIA

În afară de cazul în care operațiunea de prelucrare constituie o excepție, DPIA trebuie efectuată dacă o operațiune de prelucrare este „susceptibilă să genereze un risc ridicat" și anume:

a. unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsurăsemnificativă";

b. prelucrării pe scară largă a unor categorii speciale de date, menționată la articolul 9 alineatul (1), sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționată la articolul 10;

c. monitorizări sistematice pe scară largă a uneizone accesibile publicului.

Stabilirea dacă o prelucrare este susceptibilă să genereze un risc ridicat

1. **Evaluarea sau punctarea**, inclusiv crearea de profiluri și preconizarea în special de la aspecte privind randamentul la locul de muncă al persoanei vizate, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările.
2. **Luarea de decizii în mod automat cu un efect juridic sau similar semnificativ:** prelucrarea care are ca scop luarea deciziilor privind persoanele vizate care produc „efecte juridice privind persoana fizică" sau care „o afectează în mod similar într-o măsură semnificativă" Exemplu: prelucrarea poate conduce la excluderea sau discriminarea persoanelor.
3. **Monitorizarea sistematică:** prelucrarea utilizată pentru observarea, monitorizarea sau controlul persoanelor vizate, inclusiv datele colectate prin intermediul rețelelor sau al „unei monitorizări sistematice pe scară largă a unei zone accesibile publicului".
4. **Date sensibile sau date foarte personale**: acestea includ categorii speciale de date cu caracter personal (de exemplu, informații cu privire la opiniile politice ale persoanelor), precum și date cu caracter personal referitoare la condamnări penale sau infracțiuni. Faptul că datele cu caracter personal (imaginile video, de exemplu) sunt puse la dispoziția publicului poate fi considerat un factor în cadrul evaluării, în cazul în care se preconiza că datele urmau să fie utilizate în continuare în anumite scopuri.
5. **Datele prelucrate pe scară largă:** Se recomandă ca, în special, următorii factori să fie luați în considerare atunci când se stabilește dacă prelucrarea se

efectuează pe scară largă: numărul de persoane vizate în cauză; volumul de date și/sau gama de diferite elemente de date care sunt prelucrate; durata sau persistența activității de prelucrare a datelor și extinderea geografică a activității de prelucrare.

6. **Corelarea sau combinarea seturilor de date**, de exemplu care provin din două sau mai multe operațiuni de prelucrare a datelor efectuate în scopuri diferite și/sau de către diferiți operatori de date într-un mod care ar depăși așteptările rezonabile ale persoanei vizate.
7. **Date privind persoanele vizate vulnerabile:** prelucrarea acestui tip de date reprezintă un criteriu din cauza dezechilibrului de putere crescut dintre persoanele vizate și operatorul de date, ceea ce înseamnă că persoanele pot să nu fie în măsură a-și da consimțământul sau a respinge cu ușurință prelucrarea datelor lor sau a-și exercita drepturile.
8. **Utilizarea inovatoare sau aplicarea unor soluții tehnologice sau organizaționale noi,** cum ar fi combinarea utilizării amprentei digitale și recunoașterea facială pentru îmbunătățirea controlului accesului fizic etc.
9. **A**tunci când prelucrarea în sine „împiedică **persoanele vizate să exercite un drept sau să utilizeze un serviciu ori un contract"** Acest lucru include operațiunile de prelucrare care au ca obiectiv permiterea, modificarea sau refuzul accesului persoanelor vizate la un serviciu sau la angajarea într-un contract.

Unele dintre beneficiile efectuării unui DPIA includ:

Efectuarea unei DPIA poate îmbunătăți gradul de conștientizare a riscurilor de protecție a datelor asociate unui proiect;

- Acest lucru va ajuta organizația să îmbunătățească comunicarea privind protecția datelor cu părțile interesate relevante;
- Asigurarea și demonstrarea faptului că organizația respectă cerințele GDPR și evită sancțiunile;
- Asigurarea că angajații și clienții organizației nu riscă să le fie încălcate drepturile de protecție a datelor;
- Reducerea costurilor operaționale prin optimizarea fluxurilor de informații în cadrul unui proiect și eliminarea colectării și prelucrării inutile a datelor;
- Inspirarea încrederii clienților prin îmbunătățirea comunicărilor cu privire la problemele de protecție a datelor.
- Esențial pentru creșterea gradului de conștientizare a confidențialității între organizații.
- Un sprijin excelent acordat evaluatorilor de risc la securitatea fizică și proiectanților sistemelor de securitate (SSV) care au obligații legale pe care trebuie să le respecte și pe care, la rândul lor, sunt obligați să le comunice operatorului de date.

Metodologiile de efectuare a DPIA

Metodologiile de efectuare a DPIA pot fi diferite, dar criteriile sunt aceleași.

DPIA trebuie realizată „anterior prelucrării” (art. 35 (1) și art. 35 (1), Considerentele 90 și 93)[23]. Acest asptect este în concordanță cu asigurarea protecției datelor începând cu momentul conceperii și în mod implicit (art. 25 și Considerentul 78). DPIA ar trebui văzută ca un instrument pentru a ajuta la luarea deciziilor cu privire la prelucrare.

GDPR specifică conținutul minim a unui DPIA (conform art. 35 (7)), Considerentele 84 și 90), precizând următoarele:

- o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;
- o evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri;
- o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate menționate la alin. (1);
- măsurile preconizate în vedere abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentului Regulament, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor persoane interesate”.

GDPR nu precizează procesul DPIA care trebuie să fie urmat, ci permite, în schimb, operatorilor de date să introducă un cadru care completează practicile lor de lucru existente, cu condiția ca acesta să ia în considerare componentele descrise la articolul 35 alineatul (7).

Orientativ este prezentat în cele ce urmează un proces generic privind realizarea unei DPIA:

Încă nu există un standard ISO privind prelucrarea datelor cu caracter personal, dar se pot utiliza prevederile standardului ISO/IEC 29134:2017 Tehnologia informației - Tehnici de securitate - Evaluarea impactului asupra vieții private este un standard internațional care furnizează orientări pentru metodologiile utilizate pentru efectuarea unei DPIA și a standardului ISO 31000 Managementul Riscului (Procesele de management al riscului: comunicare și consultare, stabilirea contextului, evaluarea riscurilor, tratarea riscurilor, monitorizarea și revizuirea).

Metodologia propusă plecând de la prevederile standardului ISO/IEC 29134:2017 Tehnologia informației are următorii pași:

Criterii pentru o DPIA acceptabilă

Grupul de Lucru Articolul 29 propune următoarele criterii pe care operatorii de date le pot utiliza pentru a evalua dacă o DPIA sau o metodologie de realizare a unei DPIA este suficient de cuprinzătoare pentru a seconforma RGPD:

Se furnizează o descriere sistematică a prelucrării (art. 35 (7) a)):

- se ține cont de natura, domeniul de aplicare, contextul și scopurile prelucrării (Considerentul 90);
- se înregistrează datele cu caracter personal, destinatarii, și perioada pentru care datele cu caracter personal sunt stocate;
- se furnizează o descriere funcțională a operațiunii de prelucrare;
- se identifică activele pe care se bazează datele cu caracter personal (hardware, software, rețelele, persoanele, documentele pe suport hârtie sau canalele de transmitere pe suport de hârtie);
- se ține cont de respectarea codurilor de conduită aprobate (art. 35 (8));

Se evaluează necesitatea și proporționalitatea (art. 35 (7) b)):

- se determină măsurile preconizate în vederea conformării cu Regulamentul (art. 35 (7) d) și Considerentul 90), având în vedere:
- măsuri care contribuie la proporționalitatea și necesitatea prelucrării pe baza:
  - scopurilor determinate, explicite și legitime (art. 5 (1) b));
  - legalitatea prelucrării (art. 6);
  - adecvate, relevante și limitate la ceea ce este necesar (art. 5 (1) c));

- perioadă de stocare limitată (art. 5 (1) e));

- măsuri care contribuie la drepturile persoanelor vizate:
  - informațiile furnizate persoanei vizate (art. 12, 13 și 14);
  - dreptul de acces și dreptul la portabilitatea datelor (art. 15 și 20);
  - dreptul la rectificare și dreptul la ștergere (art. 16, 17 și 19);
  - dreptul la opoziție și dreptul la restricționarea prelucrării (art. 18, 19 și 21);
  - relațiile cu persoanele împuternicite de operator (art. 28);
  - garanțiile pentru transferurile internaționale (Capitolul V);
  - consultarea prealabilă (art. 36).

Se evaluează necesitatea și proporționalitatea (art. 35 (7) b)):

- se determină măsurile preconizate în vederea conformării cu Regulamentul (art. 35 (7) d) și Considerentul 90), având în vedere:
- măsuri care contribuie la proporționalitatea și necesitatea prelucrării pe baza:
  - scopurilor determinate, explicite și legitime (art. 5 (1) b));
  - legalitatea prelucrării (art. 6);
  - adecvate, relevante și limitate la ceea ce este necesar (art. 5 (1) c));
  - perioadă de stocare limitată (art. 5 (1) e));
- măsuri care contribuie la drepturile persoanelor vizate:
  - informațiile furnizate persoanei vizate (art. 12, 13 și 14);
  - dreptul de acces și dreptul la portabilitatea datelor (art. 15 și 20);
  - dreptul la rectificare și dreptul la ștergere (art. 16, 17 și 19);
  - dreptul la opoziție și dreptul la restricționarea prelucrării (art. 18, 19 și 21);
  - relațiile cu persoanele împuternicite de operator (art. 28);
  - garanțiile pentru transferurile internaționale (Capitolul V);
  - consultarea prealabilă (art. 36).

Se gestionează riscurile pr. drepturile și libertățile persoanelor vizate (art. 35 (7) c)):

- se analizează originea, natura, particularitatea și gravitatea riscurilor (a se vedea Considerentul 84) sau, mai exact, pentru fiecare risc (acces ilegal, modificări nedorite și dispariția datelor) din perspectiva persoanelor vizate:
  - se ține cont de sursele riscurilor (Considerentul 90);

- se identifică impactul posibil asupra drepturilor și libertăților persoanelor vizate în cazul unor evenimente ce includ accesul ilegal, modificările nedorite sau dispariția datelor;
- se identifică amenințările care ar putea conduce la accesul ilegal, modificarea nedorită sau dispariția datelor;
- se estimează probabilitatea și gravitatea (Considerentul 90);

➢ se determină măsurile preconizate pentru atenuarea respectivelor riscuri (art. 35 (7) d) și Considerentul 90);

Sunt implicate părțile interesate:

- se solicită avizul DPO (art. 35 (2));
- se solicită, acolo unde este cazul, avizul persoanelor vizate sau al reprezentanților acestora (art. 35 (9)).

BIBLIOGRAFIE

Augustin Fuerea, Aplicarea dreptului Uniunii Europene potrivit prevederilor Constituției României și ale altor norme de drept intern, Revista Dreptul, nr. 6/2019.

Roxana-Mariana Popescu, Aspecte constituționale ale integrării României în Uniunea Europeană, Revista Dreptul, nr. 3/2017.

Augustin Fuerea, Aplicarea legislației, în materia protecției datelor cu caracter personal, de către practicienii în insolvență, Revista Universul Juridic, nr. 12/2020.

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 privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:02016R0679-20160504.

Henri Oberdorff, Nouveaux outils, nouveaux acteur: vers une cybercitoyenneté ?, volumul ”Le monde quivient. Entrepérils et promesses. 2000-2015: un état des droits”, coordonatori G. Aschieri, J.-P. Dubois, E. Tartakowsky, P. Tartakowsky, Éditions La Découverte, Paris, 2016.

Cécile de Terwangne, Internet et la protection de la vie privées des données à caractère personnel, în volumul “L’Europe des droits de l’homme à l’heure d’Internet” de Quentin van Enis şi Cécile de Terwangne (dir.), Éditions Bruylant, Bruxelles, 2019.

Recomandarea CM/Rec (2010) 13 din 23 noiembrie 2010 a Comitetului de Miniştri al Consiliului Europei asupra protecţiei persoanelor cu privire la prelucrarea automată a datelor cu caracter personal în cadrul creării de profiluri.

[1]C.J.U.E., Marea Cameră, 8 aprilie 2014, Digital Rights Ireland, aff. jointes C-293/12 şi C-594/12 în ibidem, inclusiv nota de subsol nr. 23. Directiva 2006/24/CE a Parlamentului European şi a Consiliului, din 15 martie 2006, publicată în J.O.U.E., L. 105.

J. Rochfeld, L’identité numérique en Europe, în E. Pataut (coord.), L’identité à l’épreuve de la mondialisation, Editura Institut de recherche juridique de la Sorbonne, 2016.

Curtea constituțională federală a Germaniei a statuat în data de 15 decembrie 1983 dreptul la „Informationelle Selbstbestimmung”, adică la „auto-determinare informațională”, apud. J. Rochfeld, L’identité.

Voroneanu Carmen, Aspecte de ordin practic privind implementarea cerinţelor "Regulamentului general privind protecţia datelor" (RGPD) în biblioteci, An 32 Nr. 52021 https://www.bibnat.ro/dyn-doc/publicatii/Revista Biblioteca 5_2021_site.pdf.

Sava Ruxandra, Regulamentul General privind Protecţia Datelor (RGPD) pe înţelesul tău, Bucureşti Editură Universul Juridic, 2019.

Luncaşu Silviu-Cristian, Formarea şi dezvoltarea pregătirii responsabilului cu protecţia datelor cu caracter personal (DPO), în lumina noului GDPR (UE) nr. 679/2016, Bucureşti, Editură Edit Moroşan, 2018.
Șandru Daniel – Mihail, Imposibila coexistență între protecția datelor și comunitățile virtuale? Ce urmează?, Pandectele Române nr. 1/2018.

Sava Ruxandra, Când decizia o ia mașina… Despre profilare, drepturi și echilibru într-un univers digital, Revista Romana pentru Protecția și Securitatea Datelor cu Caracter Personal nr. 3/2020.

Alexe Irina, Șandru Daniel-Mihail (editori), Legislația privind protecția datelor în România, Ed. Rosetti Internațional, București, 2018, ISBN 978-6068794-90-7.