UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

„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 GENERALĂ ÎN DOMENIUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

AGENȚIA NAȚIONALĂ A FUNCȚIONARILOR PUBLICI

Acest material a fost realizat astfel:

Capitolul	Autorul
I. Legislaţie. Definiţii. Categorii de date cu caracter personal	Prof.univ.dr.Fuerea Augustin, Dr. Păcurar Gheorghe
II. Principii privind prelucrarea datelor cu caracter personal	Dr. Katona Levente, Ing. Gustea Marius
III. Modalităţi de prelucrare a datelor cu caracter personal şi drepturile persoanei vizate, în cadrul activităţilor specifice ale sistemului de coordonare, gestionare şi control al FESI	Prof.univ.dr.Rădulescu Dragoș, Av.dr. Radu Daniela
IV. Evaluarea impactului asupra protecției datelor cu caracter personal	Dr. Katona Levente, Ing. Gustea Marius
V. Măsuri/instrumente/proceduri aplicabile la nivel naţional şi European şi interdependenţa lor în domeniul specific FESI	Av. Basarabescu Georgeta, Ec. Specialist Protecția Datelor Basarabescu Cătălin
VI. Respectarea cerinţelor privind datele informatice şi securitatea sistemelor informatice, inclusiv incidența asupra funcționalității MYSMIS	Ec. Mureșan Liviu, Prof.univ.dr.Mureșan Mihaela
VII. Consecinţele nerespectării prevederilor Regulamentului General privind Protecția Datelor (GDPR)	Prof.univ.dr.Pop Stefan

C U P R I N S

CAPITOLUL I. LEGISLAŢIE. DEFINIŢII. CATEGORII DE DATE 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].

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 viața sa personală, în familia sa, în domiciliul lui sau în corespondența sa, nici la atingeri aduse onoarei şi reputației sale". Acestor mențiuni i se adaugă și cea potrivit căreia„orice persoană are dreptul la protecția 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 vieții 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 corespondenței sale". Alineatul (2) completează această dispoziție, menționând că „nu este admis amestecul unei autorități 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 națională, siguranța publică, bunăstarea economică a țării, apărarea ordinii şi prevenirea faptelor penale, protecția sănătății, a moralei, a drepturilor şi a libertăților altora".

C. Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981[2]

[1] **Augustin Fuerea**, *Invocarea excepțiilor privind protecția datelor care au caracter personal în materia executării silite,* comunicare susținută în cadrul *Conferinței* Naționale „GDPR în executarea silită", din 15 aprilie 2021. Comunicarea va fi publicată în volumul Conferinței.

[2] Ratificată de România prin Legea nr. 682/2001, publicată în Monitorul Oficial al României, Partea I, nr. 830 din 21 decembrie 2001.

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 şi libertăţilor sale fundamentale şi, în special, dreptul la viața privată, față de prelucrarea automatizată a datelor cu caracter personal care o privesc (protecția datelor)". În sensul Convenției, „datele cu caracter personal care fac obiectul unei prelucrări automatizate trebuie să fie: obţinute şi 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"[3]. În concordanță cu prevederile Convenției, „date cu caracter personal reprezintă orice informaţie privind persoana fizică identificată sau identificabilă (persoană vizată)"[4].

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. 39 TUE, similar art. 16 TFUE, precizează că „respectarea acestor norme face obiectul controlului unor autorități independente"[5].

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

[3] Art. 5 din Convenție.
[4] Art. 2 lit. a).
[5] 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"

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[6], 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, dar în condițiile în care se asigură și un nivel ridicat de protecție a datelor cu caracter personal"[7].

„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

[6] 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.

[7] **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.

economice la acest nivel, denaturând concurența și împiedicând autoritățile să-și îndeplinească responsabilitățile care le revin, potrivit dreptului UE”[8].

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 excepția cazului în care Constituţia sau legile interne conţin dispoziții mai favorabile*[9]” (de ex.: Declarația Universală a Drepturilor Omului și Convenția pentru Apărarea Drepturilor Omului și a Libertăților Fundamentale);

- art. 148 alin. (2) și (4)[10] din Legea fundamentală: „ca urmare a aderării, prevederile tratatelor constitutive ale Uniunii Europene, precum şi celelalte reglementări comunitare cu caracter obligatoriu, *au prioritate față de dispozițiile contrare din legile interne, cu respectarea prevederilor actului de aderare*[11]” (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 excepția cazului în care prezentul cod conţine dispoziții mai favorabile”, respectiv „în materiile reglementate de prezentul cod, normele dreptului Uniunii Europene se aplică în mod prioritar, indiferent de calitatea sau statutul părţilor”.

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”[12] 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”[13];

„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

[8] **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.
[9] Sublinierea noastră.
[10]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.
[11] 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..
[12] Art. 3 alin. (2).
[13] Art. 4.

pentru a preveni abuzurile la care s-ar putea ajunge din partea tuturor părților aflate în astfel de raporturi”[14].

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 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:

[14] **Augustin Fuerea**, *Aplicarea legislației, în materia protecției datelor cu caracter personal, de către practicienii în insolvență,* Revista Universul Juridic, nr. 12/2020, pag. 113.

(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)”[15].

Acestora li se adaugă[16]: 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, prenumele şi numele persoanei care l-a prescris, numărul de telefon etc.), fie sub formă de prescripţie separată sau sub formă de modele extrase dintr-o serie de prescripţii, pot fi considerate drept date cu caracter personal referitoare la un medic care prescrie medicamentul, chiar dacă pacientul este anonim. Astfel, furnizarea de informaţii referitoare la prescripţiile scrise de medici identificaţi sau identificabili producătorilor de medicamente eliberate pe bază de reţetă reprezintă o comunicare a datelor cu caracter personal către destinatari terţi”*[17].

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

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

[17] 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.

- *„serviciile bancare prin telefon: În cazul serviciilor bancare prin telefon, atunci când vocea clientului care oferă instrucţiuni băncii este înregistrată, instrucţiunile respective înregistrate trebuie considerate ca date cu caracter personal”*[18].

- *„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”*[19].

- *„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 fetiţa respectivă care prezintă familia acesteia. Desenul furnizează informații cu privire la starea fetiței și 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, părinții își pot exercita dreptul de acces la această informaţie specifică”*[20].

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””[21].

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 protecție, deoarece utilizarea unor astfel de date sensibile poate avea efecte negative semnificative asupra persoanelor

[18] Exemplu preluat din *Avizul 4/2007 privind conceptul de date cu caracter personal*, adoptat la 20 iunie 2007, 01248/07/RO, WP 136, pag. 9.
[19] Exemplu preluat din *Avizul 4/2007 privind conceptul de date cu caracter personal*, adoptat la 20 iunie 2007, 01248/07/RO, WP 136, pag. 9.
[20] Exemplu preluat din *Avizul 4/2007 privind conceptul de date cu caracter personal*, adoptat la 20 iunie 2007, 01248/07/RO, WP 136, pag. 9.
[21] 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.

vizate. Având în vedere acest aspect, termenul „date privind sănătatea" trebuie interpretat în sens larg"[22].

„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)"[23].

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"[24].

„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"[25].

„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.

---

[22] 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.

[23] 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.

[24] 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. 14.

[25] 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. 15.

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”[26].

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[27]. Decizia CJUE a fost luată „în contextul în care (…) noul Regulament general privind protecția datelor [RGPD] a intrat în vigoare”[28] și se aplică „precedându-l pe cel care va fi în curând aplicabil instituțiilor UE”[29]. 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[30]”[31].

b.„Hotărârea Curții de Justiție a Uniunii Europene pronunțată în cauza ***Novak***[32], 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 cândidatului la care are, în principiu, un drept de acces”[33]. Accesul cândidatului 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[34], directivă

[26] 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.
[27] Conform *Comunicatului de presă nr. 96/18* (din 29 iunie 2018) al CJUE.
[28] Conform *Comunicatului de presă nr. 96/18* (din 29 iunie 2018) al CJUE.
[29] 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).
[30] Pentru detalii tehnice (inițiale ș.a.), a se vedea Comunicatul invocat.
[31] **Augustin Fuerea**, *Aplicarea legislației, în materia protecției datelor cu caracter personal, de către practicienii în insolvență*, Revista Universul Juridic, nr. 12/2020, pag. 116.
[32] Hotărârea Curții din 20 decembrie 2017, *Peter Nowak c./ Data Protection Commissioner*, C-434/16, EU:C:2017:994.
[33] Pct. 27 din hotărâre.
[34] Directiva 95/46/CE, *precitată*.

potrivit căreia datele cu caracter personal reunesc „orice informație referitoare la o persoană fizică identificată sau identificabilă”[35]”[36].

c. Hotărârea Curții de Justiție a Uniunii Europene „pronunțată în cauza ***C-25/17***[37], potrivit căreia „o comunitate religioasă, (...), este operator[38], 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”[39] 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 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 (...)”[40] cu privire la care dreptul UE nu s-ar aplica”[41].

B. Curtea Europeană a Drepturilor Omului

a.Hotărârea Curții Europene a Drepturilor Omului pronunțată în cauză *Bărbulescu c./România*[42]. 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”[43]. 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”[44].

b.Hotărârea Curții Europene a Drepturilor Omului „pronunțată în cauza *Libert c./Franța*[45]. 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-

[35] 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”.
[36] **Augustin Fuerea**, *Aplicarea legislației, în materia protecției datelor cu caracter personal, de către practicienii în insolvență*, Revista Universul Juridic, nr. 12/2020, pag. 116-117.
[37] Hotărârea Curții din 10 iulie 2018, *Tietosuojavaltuutettu*, C-25/17, EU:C:2018:551.
[38] 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).
[39] Potrivit pct. 75 din hotărârea pronunțată în cauza C-25/17, *precitată*.
[40]Potrivit pct. 75 din hotărârea pronunțată în cauza C-25/17, *precitată*, pct. 42.
[41]**Augustin Fuerea**, *Aplicarea legislației, în materia protecției datelor cu caracter personal, de către practicienii în insolvență*, Revista Universul Juridic, nr. 12/2020, pag. 117.
[42] Hotărârea din 5 septembrie 2017, cererea 61496/08.
[43]https://www.echr.coe.int/Documents/FS_Data_RON.pdf, accesat la 16 ianuarie 2020.
[44]**Augustin Fuerea**, *Aplicarea legislației, în materia protecției datelor cu caracter personal, de către practicienii în insolvență*, Revista Universul Juridic, nr. 12/2020, pag. 118.
[45] Hotărârea din 2 iulie 2018 (cererea 588/13).

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"[46].

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[47], în contextul sănătății[48], în procedurile din domeniul asigurărilor sociale[49], în stocarea datelor în registre secrete[50], date ale furnizorilor de servicii de telecomunicații, divulgarea datelor cu caracter personal[51], accesul la date cu caracter personal[52], ștergerea sau distrugerea datelor cu caracter personal[53]"[54].

C. Instanțe din România

a.„Tribunalul București a sesizat CJUE[55] 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"[56]. 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[57] 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[58] (art. 8 și 32). În verificarea pe care Autoritatea a realizat-o a urmărit, inclusiv, aplicarea Legii nr. 506/2004 privind

[46]**Augustin Fuerea**, *Aplicarea legislației, în materia protecției datelor cu caracter personal, de către practicienii în insolvență*, Revista Universul Juridic, nr. 12/2020, pag. 118.
[47] *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.
[48] *Chave născutăJullien c./Franța* (hotărârea din 9 iulie 1991, cererea 14461/88) ș.a.
[49] *Vukota c./Elveția* (hotărârea din 18 octombrie 2016, cererea 61838/10) ș.a.
[50] *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.
[51] *Radu c./Republica Moldova* (hotărârea din 15 aprilie 2014, cererea 50073/07) ș.a.
[52] *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.
[53] *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.
[54] **Augustin Fuerea**, *Aplicarea legislației, în materia protecției datelor cu caracter personal, de către practicienii în insolvență*, Revista Universul Juridic, nr. 12/2020, pag. 118-119.
[55] *Orange Romania SA c. / Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*, C-61/19, EU:C:2020:901.
[56]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).
[57] Aceste copii au fost luate și păstrate fără acordul expres al clienților Orange.
[58] 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.

prelucrarea rapidă a datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice[59]. 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"[60].

b. Tribunalul București a solicitat Curții de Justiție a UE interpretarea dreptului Uniunii[61] 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 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).

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 ala 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 Informații Schengen în Republica Bulgaria și în România;

---

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

[60] **Augustin Fuerea**, *Aplicarea legislației, în materia protecției datelor cu caracter personal, de către practicienii în insolvență*, Revista Universul Juridic, nr. 12/2020, pag. 120.

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

- ⇨ 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 Informații privind vizele (VIS) în vederea consultării de către autoritățile desemnate ale statelor membre și de către Europol în scopul prevenirii, depistării și cercetării infracțiunilor de terorism și a altor infracțiuni 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 și a altor dispoziții de aplicare a Sistemului de Informații Schengen din a doua generație (SIS II);
- ⇨ Decizia 2007/533/JAI din 27 iunie 2007 privind instituirea, funcționarea și utilizarea Sistemului de Informații Schengen din a doua generație;
- ⇨ 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.

C. Legislație internă

- ⇨ Legea nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările și completările ulterioare, republicată;
- ⇨ 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;
- ⇨ Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (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);
- ⇨ Legea nr. 363/2018 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, precum și privind libera circulație a acestor date;
- ⇨ Legea nr. 682/2001 privind ratificarea Convenției pentru protejarea persoanelor față 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 și protecția vieții private în sectorul comunicațiilor electronice;
- ⇨ Legea nr. 365/2002 privind comerțul 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 Țărilor de Jos și Republica Austria privind aprofundarea

cooperării transfrontaliere, în special în vederea combaterii terorismului, criminalității transfrontaliere şi migraţiei ilegale, semnat la Prum la 27 mai 2005;
- ⇨ Regulamentul de Organizare şi Funcţionare al ANSPDCP din 11 Noiembrie 2005, cu modificările şi completările ulterioare.

D. 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 protecțiapersoanelor 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 protecția persoanelor fizice în ceea ce privește 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 investigaţiilor;
- ⇨ Decizia nr. 174/2018 privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal.

E. 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.

F. 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 Protecția 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 Protecția Datelor.

CAPITOLUL II. PRINCIPII PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL

Considerente din Regulament ce privesc principiile de prelucrare a datelor cu caracter personal.

Principiile și normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal ar trebui, indiferent de cetățenia sau de locul de reședință al persoanelor fizice, să respecte drepturile și libertățile fundamentale ale acestora, în special dreptul la protecția datelor cu caracter personal. Prezentul regulament urmărește să contribuie la realizarea unui spațiu de libertate, securitate și justiție și a unei uniuni economice, la progresul economic și social, la consolidarea și convergența economiilor în cadrul pieței interne și la bunăstarea persoanelor fizice.

Prelucrarea datelor cu caracter personal ar trebui 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, în conformitate cu principiul proporționalității. Prezentul regulament respectă toate drepturile fundamentale și libertățile și **principiile recunoscute în cartă astfel cum sunt consacrate în tratate, în special respectarea vieții private și de familie, a reședinței și a comunicațiilor, a protecției datelor cu caracter personal, a libertății de gândire, de conștiință și de religie, a libertății de exprimare și de informare, a libertății de a desfășura o activitate comercială, dreptul la o cale de atac eficientă și la un proces echitabil, precum și diversitatea culturală, religioasă și lingvistică.**

Principiile protecției datelor ar trebui să se aplice oricărei informații referitoare la o persoană fizică identificată sau identificabilă. Datele cu caracter personal care au fost supuse pseudonimizării, care ar putea fi atribuite unei persoane fizice prin utilizarea de informații suplimentare, ar trebui considerate informații referitoare la o persoană fizică identificabilă. Pentru a se determina dacă o persoană fizică este identificabilă, ar trebui să se ia în considerare toate mijloacele, cum ar fi individualizarea, pe care este probabil, în mod rezonabil, să le utilizeze fie operatorul, fie o altă persoană, în scopul identificării, în mod direct sau indirect, a persoanei fizice respective. Pentru a se determina dacă este probabil, în mod rezonabil, să fie utilizate mijloace pentru identificarea persoanei fizice, ar trebui luați în considerare toți factorii obiectivi, precum costurile și intervalul de timp necesare pentru identificare, ținându-se seama atât de tehnologia disponibilă la momentul prelucrării, cât și de dezvoltarea tehnologică. **Principiile protecției datelor ar trebui, prin urmare, să nu se aplice informațiilor anonime, adică informațiilor care nu sunt legate de o persoană fizică identificată sau identificabilă sau datelor cu caracter personal care sunt anonimizate astfel încât persoana vizată nu este sau nu mai este identificabilă.** Prin urmare, prezentul

regulament nu se aplică prelucrării unor astfel de informații anonime, inclusiv în cazul în care acestea sunt utilizate în scopuri statistice sau de cercetare.

Prelucrarea datelor cu caracter personal în alte scopuri decât scopurile pentru care datele cu caracter personal au fost inițial colectate ar trebui să fie permisă doar atunci când prelucrarea este compatibilă cu scopurile respective pentru care datele cu caracter personal au fost inițial colectate. În acest caz nu este necesar un temei juridic separat de cel pe baza căruia a fost permisă colectarea datelor cu caracter personal. În cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul, dreptul Uniunii sau dreptul intern poate stabili și specifica sarcinile și scopurile pentru care prelucrarea ulterioară ar trebui considerată a fi compatibilă și legală. Prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice ar trebui considerată ca reprezentând operațiuni de prelucrare legale compatibile. Temeiul juridic prevăzut în dreptul Uniunii sau în dreptul intern pentru prelucrarea datelor cu caracter personal poate constitui, de asemenea, un temei juridic pentru prelucrarea ulterioară. Pentru a stabili dacă scopul prelucrării ulterioare este compatibil cu scopul pentru care au fost colectate inițial datele cu caracter personal, operatorul, după ce a îndeplinit toate cerințele privind legalitatea prelucrării inițiale, ar trebui să țină seama, printre altele, de orice legătură între respectivele scopuri și scopurile prelucrării ulterioare preconizate, de contextul în care au fost colectate datele cu caracter personal, în special de așteptările rezonabile ale persoanelor vizate, bazate pe relația lor cu operatorul, în ceea ce privește utilizarea ulterioară a datelor, de natura datelor cu caracter personal, de consecințele prelucrării ulterioare preconizate asupra persoanelor vizate, precum și de existența garanțiilor corespunzătoare atât în cadrul operațiunilor de prelucrare inițiale, cât și în cadrul operațiunilor de prelucrare ulterioare preconizate. În cazul în care persoana vizată și-a dat consimțământul sau prelucrarea se bazează pe dreptul Uniunii sau pe dreptul intern, care constituie o măsură necesară și proporțională într-o societate democratică pentru a proteja, în special, obiective importante de interes public general, operatorul ar trebui să aibă posibilitatea de a prelucra în continuare datele cu caracter personal, indiferent de compatibilitatea scopurilor**. În orice caz, aplicarea principiilor stabilite de prezentul regulament și, în special, informarea persoanei vizate cu privire la aceste alte scopuri și la drepturile sale, inclusiv dreptul la opoziție, ar trebui să fie garantate.** Indicarea unor posibile infracțiuni sau amenințări la adresa siguranței publice de către operator și transmiterea către o autoritate competentă a datelor cu caracter personal relevante în cazuri individuale sau în mai multe cazuri legate de aceeași infracțiune sau de aceleași amenințări la adresa siguranței publice ar trebui considerată ca fiind în interesul legitim urmărit de operator. Cu toate acestea, o astfel de transmitere în interesul legitim al operatorului sau prelucrarea ulterioară a datelor cu caracter personal ar trebui interzisă în cazul în care prelucrarea nu este compatibilă cu o obligație legală, profesională sau cu o altă obligație de păstrare a confidențialității.

Conform principiilor prelucrării echitabile și transparente, persoana vizată este informată cu privire la existența unei operațiuni de prelucrare și la scopurile acesteia. Operatorul ar trebui să furnizeze persoanei vizate orice informații suplimentare necesare pentru a asigura o prelucrare echitabilă și transparentă, ținând seama de circumstanțele specifice și de contextul în care sunt prelucrate datele cu caracter personal. În plus, persoana vizată ar trebui informată cu privire la crearea de profiluri, precum și la consecințele acesteia. Atunci când datele cu caracter personal sunt colectate de la persoana vizată, aceasta ar trebui informată, de asemenea, dacă are obligația de a furniza

datele cu caracter personal și care sunt consecințele în cazul unui refuz. Aceste informații pot fi furnizate în combinație cu pictograme standardizate pentru a oferi într-un mod ușor vizibil, inteligibil și clar lizibil o imagine de ansamblu semnificativă asupra prelucrării avute în vedere. În cazul în care pictogramele sunt prezentate în format electronic, acestea ar trebui să poată fi citite automat.

(72) Crearea de profiluri este supusă normelor prezentului regulament care reglementează prelucrarea datelor cu caracter personal, precum temeiurile juridice ale prelucrării **sau principiile de protecție a datelor.** Comitetul european pentru protecția datelor instituit prin prezentul regulament („comitetul") ar trebui să poată emite orientări în acest context.

Dreptul Uniunii sau dreptul intern poate impune restricții în privința unor principii specifice, în privința dreptului de informare, a dreptului de acces la datele cu caracter personal și de rectificare sau ștergere a acestora, în privința dreptului la portabilitatea datelor, a dreptului la opoziție, a deciziilor bazate pe crearea de profiluri, precum și în privința comunicării unei încălcări a securității datelor cu caracter personal persoanei vizate și a anumitor obligații conexe ale operatorilor, în măsura în care acest lucru este necesar și proporțional într-o societate democratică pentru a se garanta siguranța publică, inclusiv protecția vieții oamenilor, în special ca răspuns la dezastre naturale sau provocate de om, prevenirea, investigarea și urmărirea penală a infracțiunilor sau executarea pedepselor, inclusiv protejarea împotriva amenințărilor la adresa siguranței publice sau împotriva încălcării eticii în cazul profesiilor reglementate și prevenirea acestora, alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, menținerea de registre publice din motive de interes public general, prelucrarea ulterioară a datelor cu caracter personal arhivate pentru a transmite informații specifice legate de comportamentul politic în perioada regimurilor fostelor state totalitare, protecția persoanei vizate sau a drepturilor și libertăților unor terți, inclusiv protecția socială, sănătatea publică și scopurile umanitare. Aceste restricții ar trebui să fie conforme cu cerințele prevăzute de cartă și de Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale.

(110) Un grup de întreprinderi sau un grup de întreprinderi implicat într-o activitate economică comună ar trebui să poată utiliza regulile corporatiste obligatorii aprobate pentru transferurile sale internaționale dinspre Uniune către organizații din cadrul aceluiași grup de întreprinderi sau grup de întreprinderi implicate într-o activitate economică comună, cu condiția ca astfel de reguli corporatiste **să includă toate principiile esențiale și drepturile opozabile în scopul asigurării unor garanții adecvate pentru transferurile sau categoriile de transferuri de date cu caracter personal.**

Pentru a consolida respectarea aplicării normelor prevăzute în prezentul regulament, ar trebui impuse sancțiuni, inclusiv amenzi administrative, pentru orice încălcare a prezentului regulament, pe lângă sau în locul măsurilor adecvate impuse de autoritatea de supraveghere în temeiul prezentului regulament. În cazul unei încălcări minore sau în cazul în care amenda susceptibilă de a fi impusă ar constitui o sarcină disproporționată pentru o persoană fizică, poate fi emis un avertisment în locul unei amenzi. Cu toate acestea, ar trebui să se ia în considerare în mod corespunzător natura, gravitatea și durata încălcării, caracterul deliberat al încălcării, acțiunile întreprinse pentru a reduce prejudiciul cauzat, gradul de răspundere sau orice încălcări anterioare

relevante, modul în care încălcarea a fost adusă la cunoștința autorității de supraveghere, conformitatea cu măsurile adoptate împotriva operatorului sau a persoanei împuternicite de operator, aderarea la un cod de conduită și orice alt factor agravant sau atenuant. Impunerea de sancțiuni, inclusiv de amenzi administrative, ar trebui să facă obiectul unor garanții procedurale adecvate, **în conformitate cu principiile generale ale dreptului Uniunii și cu carta, inclusiv o protecție judiciară eficientă și un proces echitabil.**

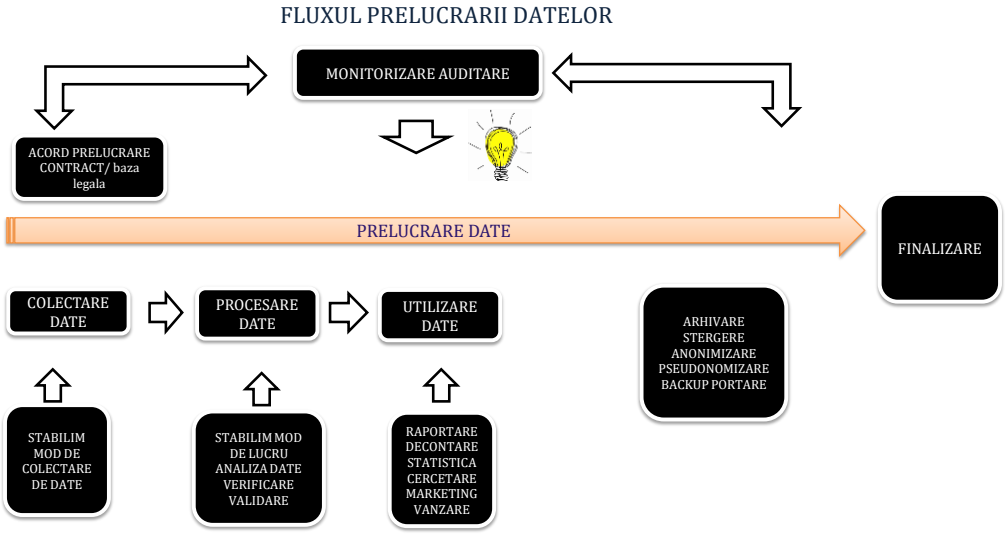
Prelucrarea datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice ar trebui să facă obiectul unor garanții adecvate pentru drepturile și libertățile persoanei vizate în temeiul prezentului regulament. Respectivele garanții ar trebui să asigure faptul că au fost instituite măsuri tehnice și organizatorice necesare pentru a se asigura, în special, principiul reducerii la minimum a datelor. Prelucrarea ulterioară a datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice se efectuează atunci când operatorul a evaluat fezabilitatea pentru îndeplinirea acestor obiective prin prelucrarea unor date cu caracter personal care nu permit sau nu mai permit identificarea persoanelor vizate, cu condiția să existe garanții adecvate (cum ar fi pseudonimizarea datelor cu caracter personal). Statele membre ar trebui să prevadă garanții adecvate pentru prelucrarea datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice. Statele membre ar trebui să fie autorizate să ofere, în anumite condiții și sub rezerva unor garanții adecvate pentru persoanele vizate, precizări și derogări în ceea ce privește cererile de informații și dreptul la rectificare, dreptul la ștergere, dreptul de a fi uitat, dreptul la restricționarea prelucrării, dreptul la portabilitatea datelor, precum și dreptul la opoziție în cazul prelucrării datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice. **Condițiile și garanțiile în cauză pot genera proceduri specifice astfel încât persoanele vizate să își exercite respectivele drepturi dacă acest lucru este adecvat în contextul scopurilor vizate de prelucrarea specifică, precum și măsuri tehnice și organizaționale vizând reducerea la minimum a prelucrării datelor cu caracter personal, în conformitate cu principiile proporționalității și necesității. Prelucrarea datelor cu caracter personal în scopuri științifice ar trebui să fie, de asemenea, conformă cu alte acte legislative relevante, cum ar fi cele privind studiile clinice.**

RGPD consacră următoarele principii ferme, sub auspiciile cărora este concepută prelucrarea datelor cu caracter personal:

- **Principiul legalității, echității si transparenței** (datele cu caracter personal sunt prelucrate în mod legal, echitabil și transparent față de persoana vizată);
- **Principiul limitării legate de scop** – evocă faptul că datele cu caracter personal sunt colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; totuși, prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată a fi incompatibilă cu scopurile inițiale;
- **Principiul limitării legate de stocare** – semnifică faptul că datele cu caracter personal trebuie păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesarăîndeplinirii scopurilor în care sunt prelucrate datele; cu toate acestea, legiuitorul european stabilește în mod expres că 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, sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric menite a garanta drepturile și libertățile persoanei vizate;

- **Principiul reducerii la minimum a datelor**, în sensul că datele cu caracter personal trebuie să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate;
- **Principiul exactității**, constând în aceea că datele cu caracter personal trebuie să fie exacte și, ori de câte ori se impune, ele trebuie să fie actualizate; ca atare, operatorul sau persoana împuternicită de operator are obligația de a lua toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile în care sunt prelucrate, sunt șterse sau rectificate fărăîntârziere;
- **Principiul integrității și confidențialității**, care impune prelucrarea într-un mod ce 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 adoptarea de măsuri tehnice sau organizatorice corespunzătoare;
- **Principiul responsabilității**, care relevă obligația operatorului de a asigura deplina conformitate a prelucrării datelor cu caracter personal cu dispozițiile RGPD, a căror respectare trebuie s-o demonstreze în permanență.



Legalitatea prelucrării datelor cu caracter personal

Suntem în prezența unei prelucrări legale a datelor cu caracter personal ori de câte ori este aplicată minimum una dintre următoarele condiții:

- persoana vizată și-a exprimat în mod valabil consimțământul pentru ca datele sale să fie prelucrate în unul sau mai multe scopuri specifice;

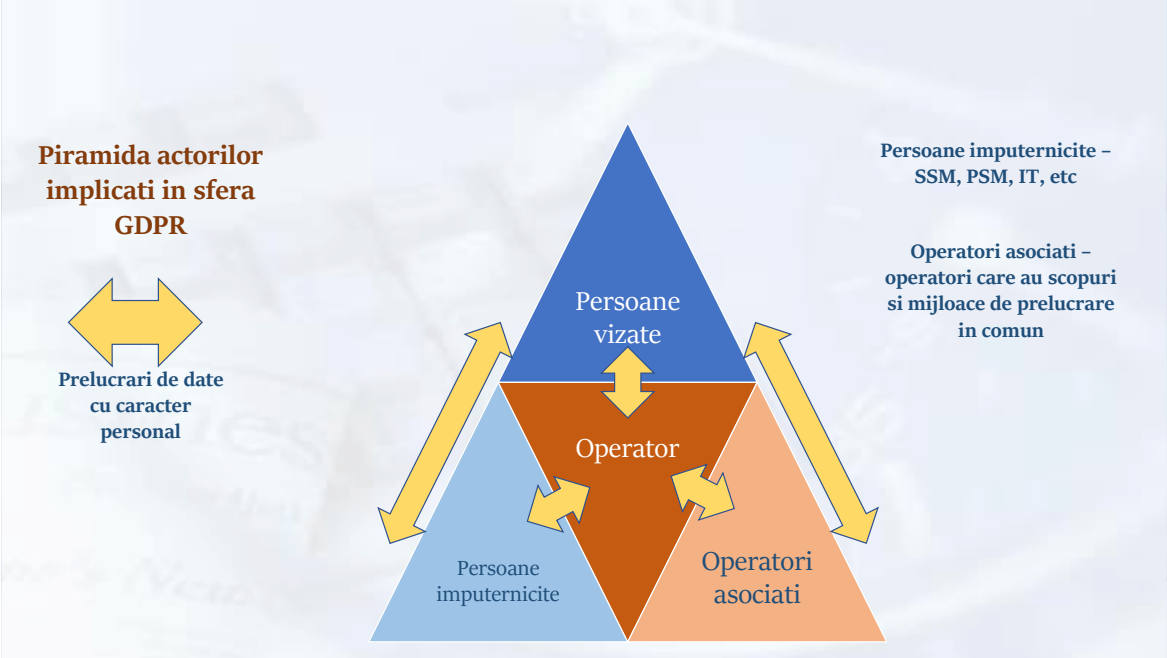
- prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru ca operatorul să facă demersuri, la cererea persoanei vizate, înainte de încheierea unui contract;
- prelucrarea este necesară în vederea îndeplinirii unei obligații legale ce îi revine operatorului;
- prelucrarea este necesară pentru protejarea intereselor 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 satisfacerii intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale alepersoanei vizate, care necesită protejarea datelor cu caracter personal, îndeosebi atunci când persoana vizată este un minor. Totuși, prin excepție, îndeplinirea acestei ultime condiții este inoperantă în situația prelucrării efectuate de autorități publice în îndeplinirea atribuțiilor lor specifice.

Scopul prelucrării datelor cu caracter personal este stabilit în baza temeiului juridic (dreptul UE sau dreptul intern aplicabil operatorului) sau, după caz, este justificat pentru îndeplinirea unei sarcini efectuate în interes public ori în cadrul exercitării unei funcții publice atribuite operatorului. Temeiul juridic poate conține dispoziții specifice privind adaptarea aplicării dispozițiilor RGPD, referitoare la: condițiile generale care reglementează legalitatea prelucrării de către operator; tipurile de date ce formează obiectul prelucrării; persoanele vizate; entitățile cărora le pot fi divulgate datele cu caracter personal și scopul divulgării acestor date; limitările legate de scop; perioadele de stocare; operațiunile și procedurile de prelucrare, inclusiv măsurile de asigurare a unei prelucrări legale și echitabile precum cele pentru alte situații speciale concrete de prelucrare (prelucrarea în contextul libertății de exprimare și de informare, prelucrarea raportată la accesul public la documente oficiale, prelucrarea unui număr de identificare național, prelucrarea în contextul ocupării unui loc de muncă, prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, asigurarea protecției datelor pentru biserici și asociații religioase). Important de reținut este faptul că atât dreptul UE, cât și dreptul intern urmăresc un obiectiv de interes public și asigură proporționalitatea cu obiectivul legitim vizat.

În situația în care prelucrarea într-un alt scop decât cel inițial pentru care datele cu caracter personal au fost colectate nu este fundamentată pe consimțământul persoanei vizate sau pe dreptul UE ori pe dreptul intern, care constituie o măsură necesarăși proporțională într-o societate democratică pentru a proteja obiective legate de securitatea națională, apărarea națională, ordinea publică, interesele majore ale UE, procedurile judiciare și sistemul judiciar, autoritatea publică, statutul profesiilor reglementate, drepturile și libertățile fundamentale și interesele vitale ale persoanelor, operatorul, pentru a stabili dacă prelucrarea în alt scop este compatibilă cu scopul pentru care datele cu caracter personal au fost colectate inițial, va lua în considerare, în mod obligatoriu, următoarele aspecte:

- 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 prin prisma relației dintre persoanele vizate și operator;

- **natura datelor cu caracter personal**, îndeosebi în cazul prelucrării unor categorii speciale de astfel de date sau în situația 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.



Consimțământul persoanei vizate pentru prelucrarea datelor cu caracter personal

În cazul în care prelucrarea se bazează pe consimțământ, operatorul trebuie să fie în măsură să demonstreze că persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal. Consimțământul trebuie sa fie exprimat clar, fără niciun fel de ambiguități, în deplină cunoștință de cauză, fără nici un fel de viciere prin eroare, dol sau violență. Lipsa unei manifestări clare de acord nu poate fi privită ca o formă de exprimare a consimțământului (ex. – în cazul căsuțelor bifate ale unui formular, prin care este prestabilit acordul, nu poate fi prezumat un consimțământ exprimat în deplină cunoștință de cauză).

În ipoteza în care consimțământul persoanei vizate este dat în contextul unei declarații scrise care se referă și la alte aspecte, cererea privind consimțământul trebuie să fie prezentată într-o formă care o diferențiază în mod clar de celelalte aspecte, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu. Nicio parte a declarației respective, care constituie o încălcare a RGPD, nu este obligatorie.

Persoana vizată are dreptul să își retragă oricând consimțământul, fără ca această retragere să afecteze legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia. Prin urmare, funcționează pe deplin, în mod firesc, principiul neretroactivității. Înainte de acordarea consimțământului, persoana vizată este informată

cu privire la acest lucru. Retragerea consimțământului se face la fel de simplu ca și acordarea acestuia.

Atunci când se evaluează dacă suntem în prezența unui consimțământ liber exprimat, se va ține seama cât mai mult de faptul că executarea unui contract, inclusiv prestarea unui serviciu, este condiționată sau nu de consimțământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract.

În situația exprimării consimțământului pentru prelucrarea datelor într-unul sau mai multe scopuri specifice, în contextul oferirii de servicii ale societății informaționale în mod direct unui minor, prelucrarea datelor copilului este legală dacă acesta are cel puțin vârsta de 16 ani. Dacă minorul are vârsta sub 16 ani, prelucrarea datelor este legală numai dacă și în măsura în care consimțământul este acordat sau autorizat de titularul răspunderii părintești asupra copilului. RGPD lasă la latitudinea statelor membre UE posibilitatea dispensei, în sensul că acestea pot să prevadă în legislația internă o vârstă inferioară în aceste scopuri, cu condiția ca acea vârstă inferioară să nu fie mai mică de 13 ani. Cu toate acestea, nu este afectat dreptul general al contractelor aplicabil în statele membre UE, în privința normelor referitoare la valabilitatea, încheierea sau efectele unui contract în legătură cu un copil.

Operatorul are obligația de a depune toate diligențele necesare pentru a stabili în asemenea cazuri că titularul răspunderii părintești a acordat sau a autorizat consimțământul, ținând cont de tehnologiile disponibile.

Prelucrarea de categorii speciale de date cu caracter personal și a datelor cu caracter personal referitoare la condamnări penale și infracțiuni:

În conformitate cu prevederile art. 9 alin. (1) din RGPD, **este interzisă prelucrarea datelor cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice ori apartenența la sindicate si 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.** Interdicția menționată nu este însă operantă în următoarele situații alternative:

- persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepția cazului în care dreptul UE sau dreptul intern prevede că interdicția de prelucrare nu poate fi ridicată chiar și in ipoteza existenței consimțământului valabil exprimat de persoana vizată;
- prelucrarea datelor este necesară în scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă și al securității sociale și protecției sociale, în măsura în care acest lucru este autorizat de dreptul UE sau de dreptul intern ori de un acord colectiv de muncă încheiat în temeiul dreptului intern, care prevede garanții adecvate pentru drepturile fundamentale și interesele persoanei vizate;
- prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul;

- prelucrarea este efectuată în cadrul activităților lor legitime și cu garanții adecvate de către o fundație, o asociație sau orice alt organism fără scop lucrativ și cu specific politic, filozofic, religios sau sindical, cu condiția ca prelucrarea să se refere numai la membrii sau la foștii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale și ca datele cu caracter personal să nu fie comunicate terților fără consimțământul persoanelor vizate;
- prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;
- prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept in instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare;
- prelucrarea este necesară din motive de interes public major, în baza dreptului UE sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamantale și a intereselor persoanei vizate;
- prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială ori a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială, în temeiul dreptului UE sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical și sub rezerva păstrării depline a secretului profesional și/sau a obligațiilor de confidențialitate specifice;
- prelucrarea este necesară din motive de interes public în domeniul sănătății publice, cum ar fi protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor și dispozitivelor medicale, în temeiul dreptului UE sau al dreptului intern, ce prevede măsuri adecvate și specifice pentru protejarea drepturilor și libertăților persoanei vizate, în special a secretului profesional;
- prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în baza dreptului UE sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanelor vizate.

Datele cu caracter personal din categoriile speciale pot fi prelucrate în scopuri legate de asistența medicală sau socială de către un profesionist supus obligației de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului UE sau al dreptului intern ori în temeiul normelor stabilite de organisme naționale competente sau de o altă persoană supusă, de asemenea, unei obligații de confidențialitate în temeiul dreptului UE sau al dreptului intern ori al normelor stabilite de organisme naționale competente.

Prelucrarea de date cu caracter personal referitoare la condamnări penale si infracțiuni sau la măsuri judiciare ori de securitate conexe se efectuează numai sub controlul unei autorități de stat sau atunci când prelucrarea este autorizată de dreptul UE sau de dreptul intern care prevede garanții adecvate pentru drepturile si libertățile persoanelor vizate. Orice registru cuprinzător al condamnărilor penale se ține numai sub controlul unei autorități de stat.

CAPITOLUL III.MODALITĂŢI DE PRELUCRARE A DATELOR CU CARACTER PERSONAL ŞI DREPTURILE PERSOANEI VIZATE, ÎN CADRUL ACTIVITĂŢILOR SPECIFICE ALE SISTEMULUI DE COORDONARE, GESTIONARE ŞI CONTROL AL FESI

Principiile protecției datelor ar trebui să se aplice oricărei informații referitoare la o persoană fizică identificată sau identificabilă.

Datele cu caracter personal care au fost supuse pseudonimizării, care ar putea fi atribuite unei persoane fizice prin utilizarea de informații suplimentare, ar trebui considerate informații referitoare la o persoană fizică identificabilă.

Pentru a se determina dacă o persoană fizică este identificabilă, ar trebui să se ia în considerare toate mijloacele, cum ar fi individualizarea, pe care este probabil, în mod rezonabil, să le utilizeze fie operatorul, fie o altă persoană, în scopul identificării, în mod direct sau indirect, a persoanei fizice respective.[62]

Pentru a se determina dacă este probabil, în mod rezonabil, să fie utilizate mijloace pentru identificarea persoanei fizice, ar trebui luați în considerare toți factorii obiectivi, precum costurile și intervalul de timp necesare pentru identificare, ținându-se seama atât de tehnologia disponibilă la momentul prelucrării, cât și de dezvoltarea tehnologică. Principiile protecției datelor ar trebui, prin urmare, să nu se aplice informațiilor anonime, adică informațiilor care nu sunt legate de o persoană fizică identificată sau identificabilă sau datelor cu caracter personal care sunt anonimizate astfel încât persoana vizată nu este sau nu mai este identificabilă.[63]

Prin urmare, prezentul regulament nu se aplică prelucrării unor astfel de informații anonime, inclusiv în cazul în care acestea sunt utilizate în scopuri statistice sau de cercetare. Regulamentul nu se aplică datelor cu caracter personal referitoare la persoane decedate. Statele membre pot să prevadă norme privind prelucrarea datelor cu caracter personal referitoare la persoane decedate.

Aplicarea pseudonimizării datelor cu caracter personal poate reduce riscurile pentru persoanele vizate și poate ajuta operatorii și persoanele împuternicite de aceștia să își îndeplinească obligațiile de protecție a datelor. Introducerea explicită a conceptului de „pseudonimizare” în prezentul regulament nu este destinată să împiedice alte eventuale măsuri de protecție a datelor.

Pentru a crea stimulente pentru aplicarea pseudonimizării atunci când sunt prelucrate date cu caracter personal, ar trebui să fie posibile măsuri de pseudonimizare, permițând în același timp analiza generală, în cadrul aceluiași operator atunci când operatorul a luat măsurile tehnice și organizatorice necesare pentru a se asigura că prezentul regulament este pus în aplicare în ceea ce privește respectiva prelucrare a datelor și că informațiile suplimentare pentru atribuirea datelor cu caracter personal unei

[62] Regulamentul (CE) nr. 45/2001 al Parlamentului European şi al Consiliului din 18 decembrie 2000 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, MO 2001 L 8, articolele 41-48.
[63] https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_ro.pdf

anumite persoane vizate sunt păstrate separat. Operatorul care prelucrează datele cu caracter personal ar trebui să indice persoanele autorizate din cadrul aceluiași operator.[64]

Persoanele fizice pot fi asociate cu identificatorii online furnizați de dispozitivele, aplicațiile, instrumentele și protocoalele lor, cum ar fi adresele IP, identificatorii cookie sau alți identificatori precum etichetele de identificare prin frecvențe radio. Aceștia pot lăsa urme care, în special atunci când sunt combinate cu identificatori unici și alte informații primite de servere, pot fi utilizate pentru crearea de profiluri ale persoanelor fizice și pentru identificarea lor.

Autoritățile publice cărora le sunt divulgate date cu caracter personal în conformitate cu o obligație legală în vederea exercitării funcției lor oficiale, cum ar fi autoritățile fiscale și vamale, unitățile de investigare financiară, autoritățile administrative independente sau autoritățile piețelor financiare responsabile de reglementarea și supravegherea piețelor titlurilor de valoare, nu ar trebui să fie considerate destinatari în cazul în care primesc date cu caracter personal care sunt necesare pentru efectuarea unei anumite anchete de interes general, în conformitate cu dreptul Uniunii sau cel al statelor membre.[65]

Cererile de divulgare trimise de autoritățile publice ar trebui să fie întotdeauna prezentate în scris, motivate și ocazionale și nu ar trebui să se refere la un sistem de evidență în totalitate sau să conducă la interconectarea sistemelor de evidență. Prelucrarea datelor cu caracter personal de către autoritățile publice respective ar trebui să respecte normele aplicabile în materie de protecție a datelor în conformitate cu scopurile prelucrării.

Consimțământul ar trebui acordat printr-o acțiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoștință de cauză și clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal, ca de exemplu o declarație făcută în scris, inclusiv în format electronic, sau verbal. Acesta ar putea include bifarea unei căsuțe atunci când persoana vizitează un site, alegerea parametrilor tehnici pentru serviciile societății informaționale sau orice altă declarație sau acțiune care indică în mod clar în acest context acceptarea de către persoana vizată a prelucrării propuse a datelor sale cu caracter personal.[66]

Prin urmare, absența unui răspuns, căsuțele bifate în prealabil sau absența unei acțiuni nu ar trebui să constituie un consimțământ. Consimțământul ar trebui să vizeze toate activitățile de prelucrare efectuate în același scop sau în aceleași scopuri. Dacă prelucrarea datelor se face în mai multe scopuri, consimțământul ar trebui dat pentru toate scopurile prelucrării.

[64] Daniel-Mihail Sandru , Protecția datelor cu caracter personal. Conformare. Sanctiuni GDPR, Editura Universitara, 2020, pag. 122

[65] SIMIONOVICI Daniela, CIREAȘĂ Daniela-Irina, LUNGU Cătălina, DAN Marius-Florian, GDPR aplicat. Instrument de lucru pentru implementarea Regulamentului UE 679/2016, Editura Wolters Kluwer România, 2019

[66]Nicolae-Dragos Ploesteanu, Ghid practic pentru conformare cu Regulamentul General privind Protecția Datelor. Instrument de audit, Editura Universul Juridic, 2019

În cazul în care consimțământul persoanei vizate trebuie acordat în urma unei cereri transmise pe cale electronică, cererea respectivă trebuie să fie clară și concisă și să nu perturbe în mod inutil utilizarea serviciului pentru care se acordă consimțământul.

Adesea nu este posibil, în momentul colectării datelor cu caracter personal, să se identifice pe deplin scopul prelucrării datelor în scopuri de cercetare științifică. Din acest motiv, persoanelor vizate ar trebui să li se permită să își exprime consimțământul pentru anumite domenii ale cercetării științifice atunci când sunt respectate standardele etice recunoscute pentru cercetarea științifică. Persoanele vizate ar trebui să aibă posibilitatea de a-și exprima consimțământul doar pentru anumite domenii de cercetare sau părți ale proiectelor de cercetare în măsura permisă de scopul preconizat.

Orice prelucrare de date cu caracter personal ar trebui să fie legală și echitabilă. Ar trebui să fie transparent pentru persoanele fizice că sunt colectate, utilizate, consultate sau prelucrate în alt mod datele cu caracter personal care le privesc și în ce măsură datele cu caracter personal sunt sau vor fi prelucrate. [67]

Principiul transparenței prevede că orice informații și comunicări referitoare la prelucrarea respectivelor date cu caracter personal sunt ușor accesibile și ușor de înțeles și că se utilizează un limbaj simplu și clar. Acest principiu se referă în special la informarea persoanelor vizate privind identitatea operatorului și scopurile prelucrării, precum și la oferirea de informații suplimentare, pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoanele fizice vizate și dreptul acestora de a li se confirma și comunica datele cu caracter personal care le privesc care sunt prelucrate.

Persoanele fizice ar trebui informate cu privire la riscurile, normele, garanțiile și drepturile în materie de prelucrare a datelor cu caracter personal și cu privire la modul în care să își exercite drepturile în legătură cu prelucrarea. În special, scopurile specifice în care datele cu caracter personal sunt prelucrate ar trebui să fie explicite și legitime și să fie determinate la momentul colectării datelor respective.

Datele cu caracter personal ar trebui să fie adecvate, relevante și limitate la ceea ce este necesar pentru scopurile în care sunt prelucrate. Aceasta necesită, în special, asigurarea faptului că perioada pentru care datele cu caracter personal sunt stocate este limitată strict la minimum. Datele cu caracter personal ar trebui prelucrate doar dacă scopul prelucrării nu poate fi îndeplinit în mod rezonabil prin alte mijloace. În vederea asigurării faptului că datele cu caracter personal nu sunt păstrate mai mult timp decât este necesar, ar trebui să se stabilească de către operator termene pentru ștergere sau revizuirea periodică. [68]

Ar trebui să fie luate toate măsurile rezonabile pentru a se asigura că datele cu caracter personal care sunt inexacte sunt rectificate sau șterse. Datele cu caracter personal ar trebui prelucrate într-un mod care să asigure în mod adecvat securitatea și confidențialitatea acestora, inclusiv în scopul prevenirii accesului neautorizat la acestea

[67] Nicolae-Dragos Ploesteanu, GDPR. Protecția datelor cu caracter personal. Aplicabil de la 25 mai 2018. Regulamentul general privind protecția datelor – Editie bilingva (romana-engleza), Editura Universul Juridic, 2018

[68] Revista de Protecția datelor cu caracter personal, Editura Universul juridic
https://www.dataprotectionromania.ro/bibliografie-protecția-datelor-cu-caracter-personal

sau utilizarea neautorizată a datelor cu caracter personal și a echipamentului utilizat pentru prelucrare.

Pentru ca prelucrarea datelor cu caracter personal să fie legală, aceasta ar trebui efectuată pe baza consimțământului persoanei vizate sau în temeiul unui alt motiv legitim, prevăzut de lege, fie în prezentul regulament, fie în alt act din dreptul Uniunii sau din dreptul intern, după cum se prevede în prezentul regulament, inclusiv necesitatea respectării obligațiilor legale la care este supus operatorul sau necesitatea de a executa un contract la care persoana vizată este parte sau pentru a parcurge etapele premergătoare încheierii unui contract, la solicitarea persoanei vizate.

Ori de câte ori regulamentul face trimitere la un temei juridic sau la o măsură legislativă, aceasta nu necesită neapărat un act legislativ adoptat de către un parlament, fără a aduce atingere cerințelor care decurg din ordinea constituțională a statului membru în cauză.

Cu toate acestea, un astfel de temei juridic sau o astfel de măsură legislativă ar trebui să fie clară și precisă, iar aplicarea acesteia ar trebui să fie previzibilă pentru persoanele vizate de aceasta, în conformitate cu jurisprudența Curții de Justiție a Uniunii Europene („Curtea de Justiție") și a Curții Europene a Drepturilor Omului.

În cazul în care prelucrarea se bazează pe consimțământul persoanei vizate, operatorul ar trebui să fie în măsură să demonstreze faptul că persoana vizată și-a dat consimțământul pentru operațiunea de prelucrare. În special, în contextul unei declarații scrise cu privire la un alt aspect, garanțiile ar trebui să asigure că persoana vizată este conștientă de faptul că și-a dat consimțământul și în ce măsură a făcut acest lucru.[69]

Pentru a garanta faptul că a fost acordat în mod liber, consimțământul nu ar trebui să constituie un temei juridic valabil pentru prelucrarea datelor cu caracter personal în cazul particular în care există un dezechilibru evident între persoana vizată și operator, în special în cazul în care operatorul este o autoritate publică, iar acest lucru face improbabilă acordarea consimțământului în mod liber în toate circumstanțele aferente respectivei situații particulare.

Consimțământul este considerat a nu fi acordat în mod liber în cazul în care aceasta nu permite să se acorde consimțământul separat pentru diferitele operațiuni de prelucrare a datelor cu caracter personal, deși acest lucru este adecvat în cazul particular, sau dacă executarea unui contract, inclusiv furnizarea unui serviciu, este condiționată de consimțământ, în ciuda faptului că consimțământul în cauză nu este necesar pentru executarea contractului.

Prelucrarea ar trebui să fie considerată legală în cazul în care este necesară în cadrul unui contract sau în vederea încheierii unui contract.[70]

---

[69] 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.

[70] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

În cazul în care prelucrarea este efectuată în conformitate cu o obligație legală a operatorului sau în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care face parte din exercitarea autorității publice, prelucrarea ar trebui să aibă un temei în dreptul Uniunii sau în dreptul intern. Prezentul regulament nu impune existența unei legi specifice pentru fiecare prelucrare în parte. Poate fi suficientă o singură lege drept temei pentru mai multe operațiuni de prelucrare efectuate în conformitate cu o obligație legală a operatorului sau în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care face parte din exercitarea autorității publice.

De asemenea, ar trebui ca scopul prelucrării să fie stabilit în dreptul Uniunii sau în dreptul intern. Mai mult decât atât, dreptul respectiv ar putea să specifice condițiile generale ale prezentului regulament care reglementează legalitatea prelucrării datelor cu caracter personal, să determine specificațiile pentru stabilirea operatorului, a tipului de date cu caracter personal care fac obiectul prelucrării, a persoanelor vizate, a entităților cărora le pot fi divulgate datele cu caracter personal, a limitărilor în funcție de scop, a perioadei de stocare și a altor măsuri pentru a garanta o prelucrare legală și echitabilă.

De asemenea, ar trebui să se stabilească în dreptul Uniunii sau în dreptul intern dacă operatorul care îndeplinește o sarcină care servește unui interes public sau care face parte din exercitarea autorității publice ar trebui să fie o autoritate publică sau o altă persoană fizică sau juridică guvernată de dreptul public sau, atunci când motive de interes public justifică acest lucru, inclusiv în scopuri medicale, precum sănătatea publică și protecția socială, precum și gestionarea serviciilor de asistență medicală, de dreptul privat, cum ar fi o asociație profesională.[71]

Prelucrarea datelor cu caracter personal ar trebui, de asemenea, să fie considerată legală în cazul în care este necesară în scopul asigurării protecției unui interes care este esențial pentru viața persoanei vizate sau pentru viața unei alte persoane fizice.

Prelucrarea datelor cu caracter personal care are drept temei interesele vitale ale unei alte persoane fizice ar trebui efectuată numai în cazul în care prelucrarea nu se poate baza în mod evident pe un alt temei juridic. Unele tipuri de prelucrare pot servi atât unor motive importante de interes public, cât și intereselor vitale ale persoanei vizate, de exemplu în cazul în care prelucrarea este necesară în scopuri umanitare, inclusiv în vederea monitorizării unei epidemii și a răspândirii acesteia sau în situații de urgențe umanitare, în special în situații de dezastre naturale sau provocate de om.

O primă măsura pe care o pot lua operatorii de date cu caracter personal este să identifice și să analizeze riscurile prezentate de prelucrările pe care le efectuează, astfel încat să adopte un nivel adecvat de protecție. Această măsură trebuie urmată de stabilirea unui plan de securitate a informațiilor care să cuprindă, în principal, securitatea tehnică pe plan informatic și securitatea spațiilor în care se prelucrează datele cu caracter personal ținând cont de cerințele minime de securitate.

Este necesară întocmirea unei politici de securitate sau un document echivalent și asigurarea faptului că această politică este implementată. Trebuie să fie organizate teste

[71] CoE, Protocol adițional la Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal privind autoritățile de supraveghere şi fluxurile transfrontaliere de date, CETS nr. 181, 2001. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181

regulate și revizii asupra măsurilor implementate pentru a se asigura că acestea se mențin în continuare eficiente. Când este cazul, aceste documente trebuie să fie revizuite.

Suplimentar măsurilor de natură tehnică, operatorii de date cu caracter personal trebuie să aiba în vedere și alte chestiuni conexe, cum ar fi, spre exemplu, modalitățile de acces la sistemele de evidență în vederea colectării datelor, în funcție de care se vor stabili și respecta măsurile tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal.[72]

Este necesară reglementarea în cuprinsul procedurii interne a personalului care are acces la sistemul informatic (cu atribuții corespunzătoare prevăzute în fișa postului) și modalitatea de utilizare, potrivit reglementărilor legale incidente în domeniu. De asemenea, este necesară desemnarea, în scris, a persoanei/persoanelor care vor prelucra datele personale și care trebuie să își asume răspunderea păstrarii confidențialității acestora; această listă conținând evidența acestor persoane va fi actualizată ori de câte ori se impune.

O altă măsură pe care o pot lua operatorii este să numească, în scris, persoana specializată în securitatea informației care să vegheze la prelucrarea datelor personale, inclusiv la buna funcționare a sistemelor informatice utilizate în această activitate. Trebuie luată în calcul revizuirea contractelor, care trebuie să fie actualizate potrivit cerințelor și principiilor GDPR.[73]

De asemenea, personalul care operează în sistem trebuie să fie instruit cu privire la protecția datelor cu caracter personal (recomandăm să existe proceduri scrise cu privire la modalitatea instruirii și eventual a unui document semnat de persoanele instruite care atestă acest lucru).

Operatorii trebuie să se asigure că oricine actionează cu drept de acces la datele cu caracter personal nu prelucrează date personale decât în situația în care a fost instruit cum să procedeze în acest sens (formare inițială și perfecționare continuă). Este vital ca personalul angajat din cadrul operatorului să înțeleagă importanța protejării datelor cu caracter personal, să fie familiarizat cu Politica de securitate și procedurile ce trebuie puse în practică.

Accesul în spațiile în care se află dispozitivele prin care se accesează sistemul trebuie acordat exclusiv personalului cu atribuții în acest sens, cu excepția celor care asigură mentenanța sistemului. De altfel, în contractele cu furnizorii care asigură mentenanța sistemului informatic trebuie prevăzute clauze specifice cu privire la protecția datelor cu caracter personal (clauze de confidențialitate cu privire la datele cu caracter personal).

Operatorii de date cu caracter personal trebuie să ia în considerare securitatea spațiilor în care sunt depozitate dispozitivele (calitate uși, încuietori, control acces etc.).

---

[72] Hotărârea CJUE din 24 noiembrie 2011 în cauzele comune C-468/10 şi C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) şi Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado, alineatele 28–29. https://curia.europa.eu/

[73] Directiva privind protecția datelor, considerentele 16 și 17; Hotărârea CEDO din 25 septembrie 2001 în cauza P.G. şi J.H./Regatul Unit, nr. 44787/98, punctele 59 şi 60; Hotărârea CEDO din 20 decembrie 2005 în cauza Wisse/Franța, nr. 71611/01.

Nu trebuie omis faptul că scopul Regulamentului este acela de a forța operatorii să își adapteze procesele interne și relațiile cu alții (furnizori, beneficiari, poprii salariați), să adopte măsuri organizatorice speciale și să implementeze proceduri de securitate adecvate, toate acestea pentru a asigura protecția datelor cu caracter personal.

Securitatea datelor nu se realizează numai prin implementarea echipamentelor corespunzătoare hardware şi software. Aceasta necesită şi norme organizatorice interne adecvate. Ideal, acestea ar trebui să trateze următoarele aspecte:[74]

• punerea la dispoziţia tuturor angajaţilor, periodic, a informațiilor despre normele privind securitatea datelor şi obligaţiile acestora în baza legislaţiei privind protecția datelor, în special obligațiile lor de confidenţialitate;

• distribuirea clară a responsabilităţilor şi sublinierea clară a competenţelor în materie de prelucrare a datelor, în special cu privire la deciziile de prelucrare a datelor cu caracter personal şi de transfer al datelor către terţi;

• utilizarea datelor cu caracter personal numai în conformitate cu instrucţiunile persoanei competente sau în conformitate cu normele generale puse în aplicare;

• protejarea accesului în spațiile şi la echipamentele hardware şi software ale operatorului sau ale persoanei împuternicite de către operator, inclusiv verificări ale autorizaţiei de acces;

• asigurarea faptului că autorizaţiile de acces la date cu caracter personal au fost acordate de către persoana competentă și necesită documentaţie adecvată;

• protocoale automatizate privind accesul la date cu caracter personal prin mijloace electronice și verificări periodice ale acestor protocoale prin intermediul departamentului intern de supraveghere;

• documentarea atentă pentru forme de dezvăluire, altele decât accesul automatizat la date pentru a putea demonstra că nu a fost efectuat niciun transfer ilegal.

Instruirea şi formarea adecvată a membrilor personalului în domeniul securităţii datelor reprezintă, de asemenea, o măsură importanţă de securitate efectivă. Procedurile de verificare trebuie, de asemenea, implementate pentru a garanta că măsurile adecvate nu există numai pe hârtie, ci şi în practică (cum ar fi audituri interne sau externe).

Măsurile de îmbunătăţire a nivelului de securitate al unui operator sau persoane împuternicite de către operator includ instrumente, cum ar fi responsabili de protecția datelor cu caracter personal, formarea angajaților în domeniul securităţii, audituri periodice, teste de penetrate şi mărci de calitate.[75]

[74] Regulamentul (CE) nr. 460/2004 al Parlamentului European şi al Consiliului din 10 martie 2004 privind instituirea Agenției Europene pentru Securitatea Rețelelor Informatice şi a Datelor, MO 2004 L 77.

[75] Directiva 2002/58/CE a Parlamentului European şi a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale şi protejarea confidenţialităţii în sectorul comunicaţiilor electronice, (Directiva asupra confidenţialităţii şi comunicaţiilor electronice), MO 2002 L 201, articolul 4 alineatul (3), modificată prin Directiva 2009/136/CE a Parlamentului European şi a Consiliului din 25 noiembrie 2009 de modificare a Directivei 2002/22/CE privind serviciul universal şi drepturile utilizatorilor cu privire la reţelele şi serviciile de comunicaţii electronice; Directiva 2002/58/CE privind prelucrarea datelor personale şi protejarea

Drepturile persoanei vizate în contextul prelucrării datelor cu caracter personal

Dreptul la informare a persoanei vizate

Regulamentul U.E. privind protecția datelor cu caracter personal (GDPR) oferă posibilitatea oricărui individ de a se informa asupra datelor sale personale. Acesta are dreptul să solicite informații privind scopul, temeiul legal pentru care datele sale personale sunt prelucrate, destinatarii acestor date, perioada de stocare, dacă sunt transferate către țări terțe, precum și datele de contact ale operatorului.

Operatorul este definit de Regulamentul GDPR drept „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." Cu alte cuvinte, el stabilește destinația datelor dar și modul de gestionare al acestora.

Operator poate fi un furnizor de servicii și chiar în mod surprinzător un administrator al unei pagini de facebook. Astfel, în cauza C-210/16, firma Wirtschaftsakademie oferea servicii de formare prin intermediul unei pagini pentru fani găzduite de Facebook[76]. Aceasta a fost sancționată de ULD (autoritatea de supraveghere de pe teritoriul landului Schleswig-Holstein) pentru că nici ea și nici Facebook nu informau vizitatorii paginii că colectau informații cu caracter personal ce ulterior erau prelucrate. Curtea de Justiție a Uniunii Europene a decis că noțiunea „operator" înglobează și administratorul unei pagini pentru fani găzduite pe o rețea socială. Beneficiază de dreptul la informare atât persoanele care au furnizat direct informațiile cât și indivizii de la care nu au fost obținute personal.

În cazul în care datele cu caracter personal sunt obținute direct de la persoana vizată, operatorul este obligat să furnizeze persoanei vizate cel puțin următoarele informații, cu excepția cazului în care această persoană posedă deja informațiile respective:[77]

a) identitatea operatorului și a reprezentantului acestuia, dacă este cazul;
b) scopul în care se face prelucrarea datelor;
c) informații suplimentare, precum: destinatarii sau categoriile de destinatari ai datelor; dacă furnizarea tuturor datelor cerute este obligatorie și consecințele refuzului de a le furniza; existența drepturilor prevăzute de prezenta lege pentru persoana vizată, în special a dreptului de acces, de intervenție asupra datelor și de opoziție, precum și condițiile în care pot fi exercitate;

---

confidenţialităţii în sectorul comunicaţiilor electronice şi Regulamentul (CE) nr. 2006/2004 privind cooperarea dintre autoritățile naționale însărcinate să asigure aplicarea legislației în materie de protecție a consumatorului, MO 2009 L 337.

[76] Hotărârea Curții (Marea cameră) din 5 iunie 2018 (cerere de decizie preliminară formulată de Bundesverwaltungsgericht - Germania) – Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein GmbH, JO C 260, 18.7.2016., https://curia.europa.eu/juris/documents.jsf?pro=&lgrec=en&nat=or&oqp=&lg=&dates=&language=ro&jur=C%2CT%2CF&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&num=C-210%252F16&td=%3BALL&pcs=Oor&avg=&page=1&mat=or&jge=&for=&cid=181210

[77] Hotărârea CEDO din 7 iulie 1989 în cauza Gaskin/Regatul Unit, nr. 10454/83; Hotărârea CEDO din 13 februarie 2003, în cauza Odièvre/Franţa [T], nr. 42326/98; Hotărârea CEDO din 28 aprilie 2009 în cauza K.H. şi alţii/Slovacia, nr. 32881/04; Hotărârea CEDO din 25 septembrie 2012 în cauza Godelli/Italia, nr. 33783/09.

d) orice alte informații a căror furnizare este impusă prin dispoziție a autorității de supraveghere, ținând seama de specificul prelucrării.

În cazul în care datele nu sunt obținute direct de la persoana vizată, operatorul este obligat ca, în momentul colectării datelor sau, dacă se intenționează dezvăluirea acestora către terți, cel mai târziu până în momentul primei dezvăluiri, să furnizeze persoanei vizate cel puțin următoarele informații, cu excepția cazului în care persoana vizată posedă deja informațiile respective:

a) identitatea operatorului și a reprezentantului acestuia, dacă este cazul;
b) scopul în care se face prelucrarea datelor;
c) informații suplimentare, precum: categoriile de date vizate, destinatarii sau categoriile de destinatari ai datelor, existența drepturilor prevăzute de prezenta lege pentru persoana vizată, în special a dreptului de acces, de intervenție asupra datelor și de opoziție, precum și condițiile în care pot fi exercitate;
d) orice alte informații a căror furnizare este impusă prin dispoziție a autorității de supraveghere, ținând seama de specificul prelucrării.

Dreptul de acces la date

Orice persoană vizată are dreptul de a obține de la operator, la cerere și în mod gratuit pentru o solicitare pe an, confirmarea faptului că datele care o privesc sunt sau nu sunt prelucrate de acesta.[78]

Operatorul este obligat, în situația în care prelucrează date cu caracter personal care privesc solicitantul, să comunice acestuia, împreuna cu confirmarea, cel puțin următoarele:

a) informații referitoare la scopurile prelucrării, categoriile de date avute în vedere și destinatarii sau categoriile de destinatari cărora le sunt dezvăluite datele;
b) comunicarea într-o formă inteligibilă a datelor care fac obiectul prelucrării, precum și a oricărei informații disponibile cu privire la originea datelor;
c) informații asupra principiilor de funcționare a mecanismului prin care se efectuează orice prelucrare automată a datelor care vizează persoana respectivă;
d) informații privind existența dreptului de intervenție asupra datelor și a dreptului de opoziție, precum și condițiile în care pot fi exercitate;
e) informații asupra posibilității de a consulta registrul de evidență a prelucrarilor de date cu caracter personal, de a înainta plângere către autoritatea de supraveghere, precum și de a se adresa instanței pentru atacarea deciziilor operatorului.

Persoana vizată poate solicita de la operator informațiile printr-o cerere întocmită în formă scrisă, datată și semnată. În cerere solicitantul poate arăta dacă dorește ca informațiile să îi fie comunicate la o anumită adresă, care poate fi și de poșta electronică, sau printr-un serviciu de corespondență care să asigure că predarea i se va face numai personal.[79]

[78] Hotărârea CEDO din 6 iunie 2006 în cauza Segerstedt-Wiberg şi alţii/Suedia, nr. 62332/00, punctele 89 şi 90; a se vedea şi, de exemplu, Hotărârea CEDO din 18 aprilie 2013 în cauza M.K./Franţa, nr. 19522/09.
[79] Hotărârea CEDO din 27 august 1997 în cauza M.S./Suedia, nr. 20837/92, în care datele medicale au fost comunicate fără consimţământ sau posibilitatea de opoziţie sau Hotărârea CEDO din 26 martie 1987 în cauza

Dreptul de intervenție asupra datelor (dreptul la rectificare)

Orice persoana vizată are dreptul de a obține de la operator, la cerere și în mod gratuit:

a) după caz, rectificarea, actualizarea, blocarea sau ștergerea datelor a căror prelucrare nu este conformă prezentei legi, în special a datelor incomplete sau inexacte;
b) după caz, transformarea în date anonime a datelor a căror prelucrare nu este conformă prezentei legi;
c) notificarea către terții cărora le-au fost dezvaluite datele a oricărei operațiuni efectuate, dacă această notificare nu se dovedește imposibilă sau nu presupune un efort disproporționat față de interesul legitim care ar putea fi lezat.

Dreptul la ștergere (dreptul de a fi uitat)

Acest drept este unul fundamental deoarece dă persoanelor vizate un drept de dispoziție asupra datelor cu caracter personal. Astfel, orice persoană poate cere ștergerea datelor pentru următoarele motive:

- scopul pentru care au fost colectate sau procesate a fost atins;
- persoana vizată „își retrage consimţământul pe baza căruia are loc prelucrarea și nu există niciun alt temei juridic pentru prelucrarea;”
- persoana se opune prelucrării datelor (dreptul de opoziție prevăzut de Regulamentul GDPR în art. 21) datele au fost ilegal procesate;
- există o obligație legală a operatorului prevăzută de dreptul Uniunii Europene sau de dreptul intern de a șterge aceste date;
- datele cu caracter personal au fost „colectate în legătură cu oferirea de servicii ale societăţii informaţionale menţionate la articolul 8 alineatul (1).” Articolul 8 alin. 1 se referă la prelucrarea datelor copiilor cu vârsta de 16 ani (prelucrare legală) și a celor sub 16 ani (prelucrarea este legală dacă titularul autorității părintești își dă consimțământul, în caz contrar, este ilegală).

Operatorul într-un termen rezonabil va șterge datele cu caracter personal și va informa și destinatarii acestor date despre solicitarea făcută de persoana vizată. Acesta nu este responsabil, dacă ulterior aceste date sunt reutilizate de către alți operatori, întrucât el are doar o obligație de mijloace. Operatorul va șterge datele cu caracter personal precum și orice copii ale acestora. Deși acest drept poate fi exercitat oricând, el conține anumite limitări. Astfel, prelucrarea este necesară în următoarele cazuri:

- pentru exercitarea dreptului la liberă exprimare şi la informare;
- pentru constatarea, exercitarea sau apărarea unui drept în instanţă;
- din motive de interes public în domeniul sănătăţii publice;
- în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice;
- pentru respectarea unei obligaţii legale care prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului sau pentru

Leander/Suedia, nr. 9248/81; sau Hotărârea CEDO din 10 mai 2011 în cauza Mosley/Regatul Unit, nr. 48009/08.

- îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este învestit operatorul.

Dreptul la restricționarea prelucrării

Prin intermediul acestui drept o persoană poate limita modul în care un operator îi folosește datele cu caracter personal. Cu toate acestea, dreptul nu este unul discreționar, fiind exercitat în anumite circumstanțe prevăzute de articolul 18 din Regulamentul GDPR:

- persoana vizată contestă exactitatea datelor personale- este o restricționare temporară operatorul făcând toate verificările necesare datele au fost prelucrate ilegal, iar persoana vizată se opune ștergerii și solicită restricția în schimb;
- operatorul nu mai are nevoie de datele personale dar persoana i le solicită pentru exercitarea sau apărarea dreptului în instanță;
- persoana vizată s-a opus prelucrării datelor în conformitate cu articolul 21 alineatul (1)- operatorul va verifica dacă interesul său legitim prevalează asupra interesului personal.

Operatorul poate refuza cererea de restricționare a persoanei vizate dacă este nefondată sau are caracter repetitiv.

Dreptul la portabilitatea datelor

Acest drept a fost introdus prin Regulamentul GDPR și oferă posibilitatea persoanelor vizate de a primi datele personale într-o manieră cât mai clară și structurată. În plus ele pot fi stocate și transmise ușor de la un operator la altul. Orice date furnizate pot face obiectul dreptului la portabilitate? Răspunsul este nu. Doar datele prelucrate pe bază de consimțământ dat în mod legal conform articolului 6 alineatul (1) litera (a) sau al articolului 9 alineatul (2) litera (a)-adică consimțământul dat pentru scopuri specifice și cel dat pentru executarea unui contract.

O graniță destul de fină în cazul acestui drept există atunci când datele altei persoane fac obiectul unei cereri de portabilitate. Un exemplu elocvent în acest caz ar fi e-mailul prin care cerem datele bancare ale unei altei persoane în scopul efectuării unui transfer bancar. Ar trebui furnizate aceste date sau nu? Răspunsul este că depinde de situație. S-a susținut că datele unei alte persoane pot fi furnizate persoanei care formulează o cerere și transmise unui alt organism dacă se face în scop strict personal, iar persoana face parte din anturajul persoanei vizate.

Dreptul de opoziție

Persoana vizată are dreptul de a se opune în orice moment, din motive întemeiate și legitime legate de situația sa particulară, ca date care o vizează să facă obiectul unei prelucrări, cu excepția cazurilor în care există dispoziții legale contrare. În caz de opoziție justificată prelucrarea nu mai poate viza datele în cauză.

Persoana vizată are dreptul de a se opune în orice moment, în mod gratuit și fără nici o justificare, ca datele care o vizează să fie prelucrate în scop de marketing direct, în numele operatorului sau al unui terț, sau să fie dezvaluite unor terți într-un asemenea scop.

Autoritățile publice țin evidența unor astfel de cazuri și informează periodic autoritatea de supraveghere despre modul de soluționare a lor.

Dreptul de a nu fi supus unei decizii individuale

Orice persoană are dreptul de a cere și de a obține:

a) retragerea sau anularea oricărei decizii care produce efecte juridice în privința sa, adoptată exclusiv pe baza unei prelucrări de date cu caracter personal, efectuată prin mijloace automate, destinată să evalueze unele aspecte ale personalității sale, precum competența profesionala, credibilitatea, comportamentul său ori alte asemenea aspecte;
b) reevaluarea oricărei alte decizii luate în privința sa, care o afectează în mod semnificativ, dacă decizia a fost adoptată exclusiv pe baza unei prelucrari de date care întrunește condițiile prevăzute de lege.

Respectându-se celelalte garanții prevăzute de prezenta lege, o persoană poate fi supusă unei decizii de natura celei vizate numai în următoarele situații:

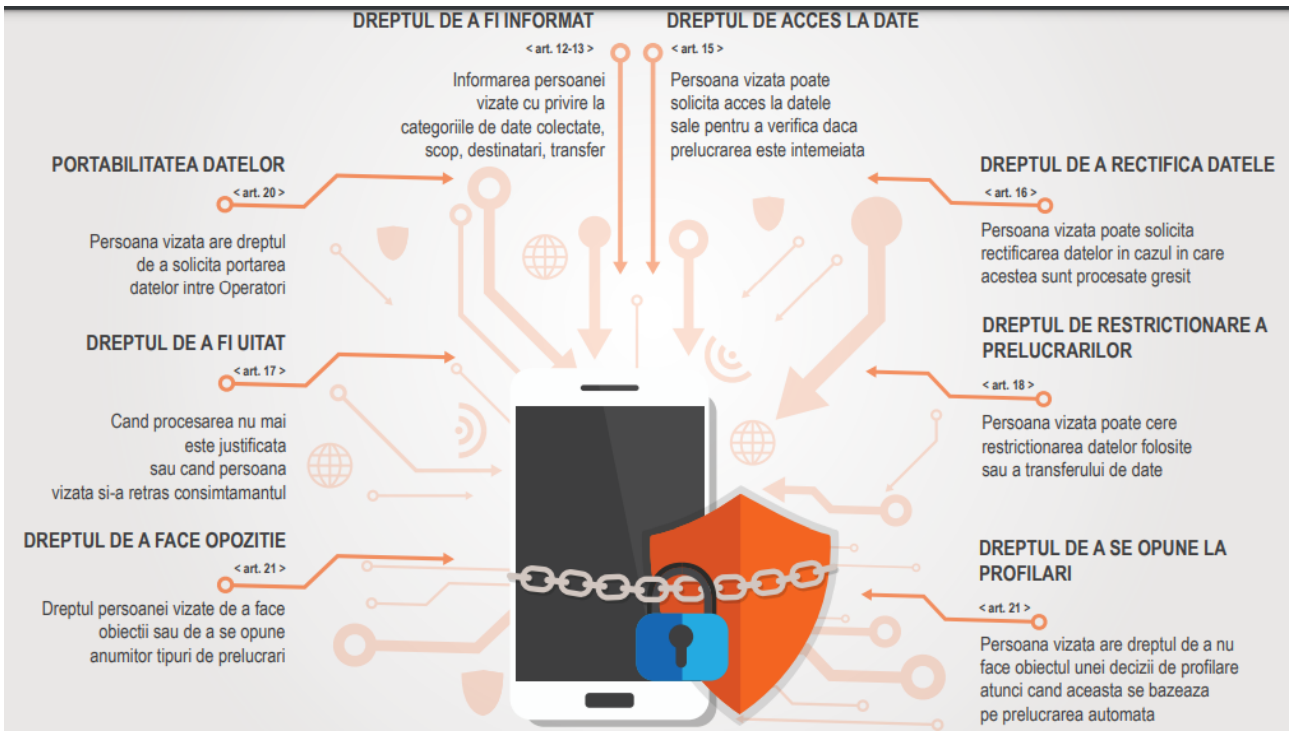
a) decizia este luată în cadrul încheierii sau executării unui contract, cu condiția ca cererea de încheiere sau de executare a contractului, introdusă de persoana vizată, să fi fost satisfacută sau ca unele măsuri adecvate, precum posibilitatea de a-și susține punctul de vedere, să garanteze apărarea propriului interes legitim;
b) decizia este autorizată de o lege care precizează măsurile ce garantează apărarea interesului legitim al persoanei vizate.

Dreptul de a se adresa justiției

Fără a se aduce atingere posibilității de a se adresa cu plângere autorității de supraveghere, persoanele vizate au dreptul de a se adresa justiției pentru apărarea oricăror drepturi garantate de prezenta lege, care le-au fost încălcate.

Orice persoană care a suferit un prejudiciu în urma unei prelucrari de date cu caracter personal, efectuată ilegal, se poate adresa instanței competente pentru repararea acestuia.

Instanța competentă este cea în a carei rază teritorială domiciliază reclamantul. Cererea de chemare în judecată este scutită de taxa de timbru.



Sursa foto:
https://accace.ro/wp-content/uploads/sites/8/2018/04/2018-04-GDPR-Infographic_V2.pdf

CAPITOLUL IV.EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR CU CARACTER PERSONAL

1. Articolul 35 Evaluarea impactului asupra protecției datelor din Regulamentul UE 679/2016
2. DECIZIE nr. 174 din 18 octombrie 2018 privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal
3. WP 248 rev.01 Ghid privind Evaluarea impactului asupra protecției datelor (DPIA) și stabilirea dacă o prelucrare este „susceptibila să genereze un risc ridicat” în sensul Regulamentului 2016/679

Articolul 35 Evaluarea impactului asupra protecției datelor

(1)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.*

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

*(3)**Evaluarea impactului asupra protecției datelor** menționată la alineatul (1) 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 măsura semnificativă;
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) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.

Repere importante de reținut:

1. Realizarea unui studiu de impact nu este obligatorie pentru fiecare operațiune de prelucrare ci doar atunci când operațiunile de prelucrare indică un risc ridicat aferent drepturilor și libertățile persoanelor fizice.
2. **Prelucrarea de date care este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice necesită DPIA** = studiu de impact.(art. 35 (1))
3. **Avizul DPO este esențial în declanșarea precum și evaluarea DPIA.**

Declarația GL 29 actuala Comisie CEPD, menționează când se evaluează analiza riscurilor și dă câteva repere despre ce înseamnă „drepturile și libertățile" persoanelor vizate:

1. drepturile la protecția datelor personale și a vieții private,
2. interzicerea discriminării,
3. libertatea de mișcare,
4. dreptul la libertate, conștiință și religie.
5. libertatea de exprimare,
6. libertatea de gândire,

Avem 2 chei de control care, când sunt îndeplinite simultan, indică necesitatea efectuării unui DPIA:

- **Riscuri majore**
- **„drepturile și libertățile" persoanelor vizate**

Ce este Riscul?

Reprezintă un scenariu care descrie un incident și consecințele pe care le produce, raportat la severitate (impact) și probabilitate.

„Managementul Riscului" se poate defini ca:

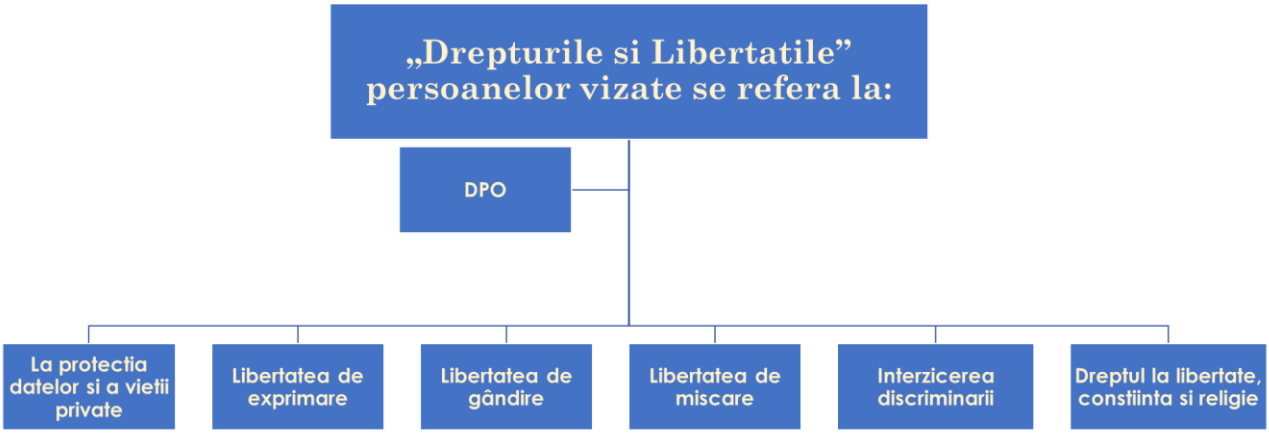
Activitățile coordonate pentru a conduce și controla o organizație cu privire la riscuri identificate.

Studiul de impact este necesar numai în cazul în care un tip de prelucrare „ar putea duce la un risc ridicat pentru drepturile și libertățile persoanelor fizice” (art. 35(1)).

Condițiile care au indicat că nu este necesar efectuarea unui studiu de impact, nu vor diminua obligațiile operatorilor de a implementa măsurile tehnico organizatorice specificate în Regulament corespunzătoare riscurilor existente asupra drepturilor și libertăților persoanelor vizate în procesul de prelucrare a datelor cu caracter personal.

Concluzionăm că există o obligativitate din partea operatorului de a monitoriza continuua ctivitățile de prelucrare:

Operatorii trebuie să desfășoare o activitate continuă de evaluare a riscurilor existente, din activitățile de prelucrare a datelor cu caracter personal, pentru a identifica când procesul poate declanșa riscuri ridicate pentru drepturile și libertățile persoanelor fizice.



Articolul 35 Evaluarea impactului asupra protecției datelor

*(4)**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**, în conformitate cu alineatul (1).*

(5)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.

*(7) **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 si proporționalității operațiunilor** de prelucrare în legătură cu aceste scopuri;*
- *c) **o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate** menționate la alineatul (1);*
- *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.

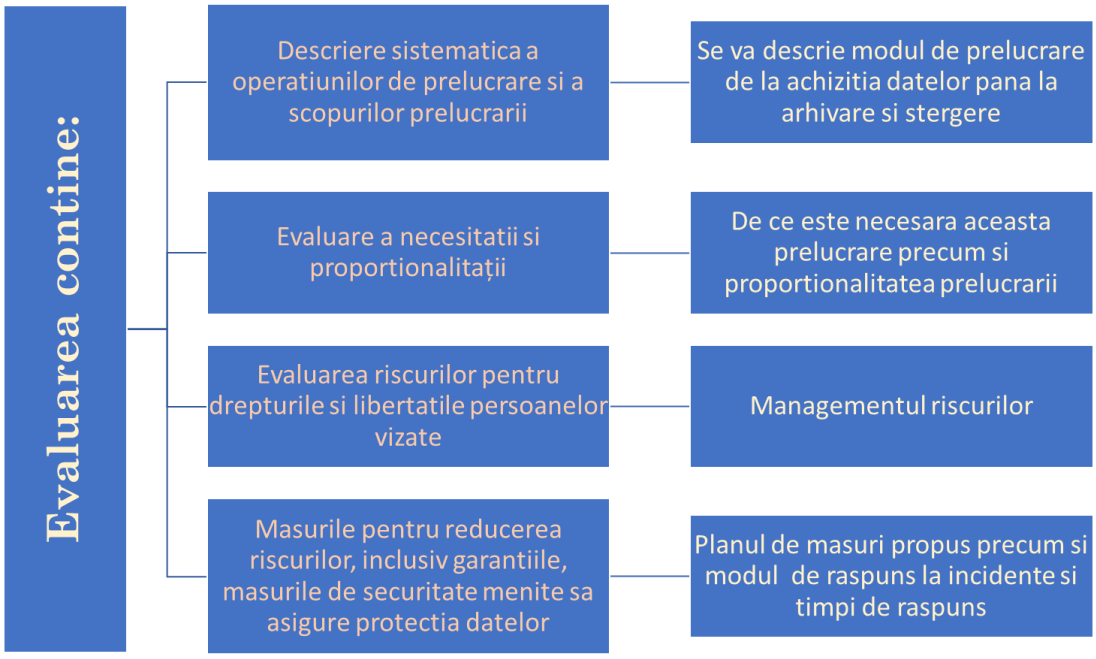
DPIA este un proces destinat să:

1. descrie prelucrarea.
2. să evalueze necesitatea și proporționalitatea acesteia
3. 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.

DPIA este un instrument esențial pentru responsabilizare, **ajută operatorii de date să respecte cerințele regulamentului și să poată demonstra că au fost luate măsuri adecvate pentru a asigura conformitatea** (conform și Art. 24).

Gestiunea riscurilor ce vizează drepturile și libertățile persoanelor fizice, necesită:

1. Să identificăm riscurile în contextul real al activităților de prelucrare;
2. Să le analizăm, să le estimăm și vom ține cont de procesul de consultare;
3. Să evaluăm corespunzător și cât mai realist aceste riscuri;
4. Să alegem corect modul de tratare (pentru atenuarea probabilității de apariție și a impactului generat);
5. Procesul de revizuire este permanent necesitând monitorizarea activității;
6. Să existe un tip de răspuns la incidente pentru limitarea pagubelor persoanelor vizate.



DECIZIE nr. 174 din 18 octombrie 2018

Art. 1

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

a) prelucrarea datelor cu caracter personal în vederea realizării 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) prelucrarea pe scară largă a datelor cu caracter personal privind originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate, a datelor genetice, a datelor biometrice pentru identificarea unică a unei persoane fizice, a datelor privind sănătatea, viața sexuală sau orientarea sexuală ale unei persoane fizice sau a datelor cu caracter personal referitoare la condamnări penale și infracțiuni;
c) 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, piețe, parcuri sau alte asemenea spații;
d) prelucrarea pe scara largă a datelor cu caracter personal ale persoanelor vulnerabile, în special ale minorilor și ale angajaților, prin mijloace automate de monitorizare și/sau înregistrare sistematică a comportamentului, inclusiv în vederea desfășurarii activităților de reclamă, marketing și publicitate;
e) prelucrarea pe scară largă a datelor cu caracter personal prin utilizarea inovatoare sau implementarea unor tehnologii noi, în special în cazul în care operațiunile respective limitează capacitatea persoanelor vizate de a-și exercita drepturile, cum ar fi utilizarea tehnicilor de recunoaștere faciala în vederea facilitării accesului în diferite spații;
f) prelucrarea pe scară largă a datelor generate de dispozitive cu senzori care transmit date prin internet sau prin alte mijloace (aplicații "Internetul lucrurilor", cum ar fi smart TV, vehicule conectate, contoare inteligente, jucării inteligente, orașe inteligente sau alte asemenea aplicații);
g) prelucrarea pe scară largă și/sau sistematică a datelor de trafic și/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 situații) atunci când prelucrarea nu este necesară pentru prestarea unui serviciu solicitat de persoana vizată.

Repere importante de reținut:

Când suntem obligați să efectuăm un DPIA (Studiu de impact)

1. Prelucrarea pe scara largă a datelor personale sensibile
2. Prelucrarea automată inclusiv crearea unor profiluri care generează efecte juridice sau o afectează în mod similar.
3. Monitorizarea sistematică pe scară largă a publicului (video, acces control)
4. Prelucrarea datelor personale ale copiilor, persoanelor vulnerabile, angajaților prin mijloace automate de monitorizare și/sau înregistrare sistematică a comportamentului.

5. Prelucrarea datelor personale cu ajutorul unor tehnologii noi, atunci când este limitat acordul persoanelor vizate (exemplu recunoaștere facială)
6. Prelucrarea datelor sensibile cu ajutorul unor dispozitive cu senzori
7. Prelucrarea sistematică a datelor de trafic și localizare, atunci când acest lucru nu este solicitat de persoana vizată.

Nerespectarea cerințelor DPIA poate conduce la aplicarea de amenzi de către autoritatea de supraveghere.

În ce condiții:

1. Nerealizarea unei DPIA atunci când prelucrarea indeplinește condițiile specificate la (art. 35 (1),(3),(4)-lista de operațiuni impuse de Autoritate).
2. Realizarea unei DPIA într-un mod incorect specificat la (art. 35 (2),(7),(9)).
3. Atunci când nu se consultă autoritatea de supraveghere, așa cum este specificat la (art. 36 (3)(e)).

Amenzile administrative pot ajunge pâna la 10 milioane EUR sau până la 2% din cifra de afaceri.

Comitetul European pentru Protecția Datelor (EDPB-CEPD) va putea emite ghiduri, recomandări și bune practici pentru a încuraja o aplicare consecventă a RGPD.art. 70 (1)(e).

Regulamentul impune operatorilor să implementeze măsuri tehnico organizatorice adecvate pentru a demonstra conformitatea, ținând cont și de „riscurile de variație a probabilității și gravității asupra drepturilor și libertăților persoanelor fizice" (art. 24(1)).

Un instrument util este analiza scalabilității procesului de prelucrare.

Categoria de operațiuni care impun un studiu de impact

O singură operațiune de prelucrare sau mai multe operațiuni similare de prelucrare pot impune un singur studiu de impact efectuat.

La art. 35 (1) se specifică că „o evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare", iar Considerentul 92 spune că „există situații ar putea fi rezonabil și util din punct de vedere economic ca o evaluare a impactului asupra protecției datelor să aiba o perspectivă mai extinsă decât cea a unui singur proiect".

Pot exista operațiuni de prelucrare „cu risc ridicat" care nu sunt cuprinse în lista specificată la art 35 (3) dar prezintă totuși riscuri la fel de mari și necesită efectuarea unui DPIA.

Expresia folosită în Regulament „în special" din expunerea art. 35 (3), indica clar că aceasta este o listă neexhaustiva.

Operatorii asociați își vor defini obligațiile ce le revin.

Studiul de impact va stabili răspunderile fiecărui operator precum și măsurile adoptate de fiecare în parte pentru a proteja drepturile și libertățile pesoanelor vizate.

Operatorii vor expune operatorilor asociați ce scopuri și necesități au, dar au dreptul de a-și proteja interesele comerciale și vulnerabilitățile organizației.

Cuvant cheie folosit în Regulament „susceptibil"

Considerentele 75, 76, 92, 116, din preambulul Regulamentului, conțin detalii care indică ce declanșează susceptibilitatea unui risc.

CEPD asociază prelucrările „sistematice" cu suspiciunea unui risc ridicat dar și prelucrările care sunt prearanjate, sau demonstrează o metodologie a prelucrării și au loc în cadrul unui plan general de colectare a datelor;

De obicei aceste metodologii fac parte din strategia operatorului de a-și desfășura activitatea și conduc în final la necesitatea efectuării unui studiu de impact pentru a proteja drepturile și libertățile persoanelor vizate.

Cele 9 criterii pentru efectuarea DPIA în opinia GL 29

1. Evaluarea sau scoring, inclusiv profilarea și preconizarea, în special din „aspecte privind performanța persoanei vizate la locul de munca, situația economică, starea de sanătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările" (Considerentele 71 si 91).

2. Proces decizional automatizat cu efecte legale sau similare semnificative: prelucrare care vizează luarea deciziilor asupra persoanelor vizate care produc:

„efecte juridice privind persoana fizică"

„o afectează în mod similar într-o masură semnificativă" (art. 35 (3) a)).

3. Monitorizare sistematică:

prelucrare folosită pentru a observa, monitoriza sau controla persoanele vizate, incluzând colectarea de date prin rețele sau „monitorizarea sistematică a unei zone accesibile publicului" (art. 35 (3) c))15.

4. Date sensibile sau date de natură foarte personală: acestea includ categorii speciale de date cu caracter personal așa cum sunt definite in art. 9 si art. 10.

5. Date prelucrate pe scară largă: RGPD nu definește ce inseamnă scara largă, însă Considerentul 91 oferă anumite linii directoare.

Grupul de Lucru Articolul 29 recomandă luarea în considerare, în special, a următorilor factori pentru a se determina dacă o prelucrare este efectuată pe scară largă:

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

6. Potrivirea sau combinarea seturilor de date, spre exemplu, provenind de la două sau mai multe operațiuni de prelucrare a datelor efectuate în scopuri diferite și/sau de diverși operatori de date într-un mod care ar depași așteptările rezonabile ale persoanei vizate.

7. Date privind persoanele vizate vulnerabile (Considerentul 75): prelucrarea acestui tip de date este un criteriu din cauza dezechilibrului de putere crescut între persoanele vizate și operator, ceea ce inseamnă că persoanele ar putea să nu fie în stare să își dea cu ușurință consimțământul sau să se opună prelucrării datelor lor sau să își exercite drepturile.

8. Utilizare inovatoare sau implementarea unor noi soluții tehnologice cum ar fi combinarea utilizării amprentei digitale cu recunoașterea facială pentru îmbunătățirea controlului accesului fizic etc.

RGPD clarifică (art. 35 (1) și Considerentele 89 si 91) faptul că utilizarea unei noi tehnologii, definită în „conformitate cu nivelul atins al cunoștințelor tehnologice" (Considerentul 91), poate declanșa necesitatea realizării unei DPIA.

Consecințele personale și sociale ale desfășurării unei noi tehnologii pot fi necunoscute.

9. Atunci când prelucrarea în sine „împiedica persoanele fizice să-și exercite un drept sau să utilizeze un serviciu sau un contract" (art. 22 si Considerentul 91).

Acestea includ operațiuni de prelucrare care vizează permiterea, modificarea sau refuzarea accesului persoanelor fizice la un serviciu, încheierea unui contract.

DPIA nu este necesară pentru operațiunile de prelucrare ce au fost deja verificate de autoritatea de supraveghere, în conformitate cu art. 20 din Directiva 95/46/CE și care sunt realizate într-un mod ce nu a suferit modificări de la verificarea prealabilă.

Într-adevar, „Deciziile adoptate ale Comisiei și autorizațiile autorităților de supraveghere emise pe baza Directivei 95/46/CE ramân în vigoare pâna când vor fi modificate, înlocuite sau abrogate" (Considerentul 171).

În ce moment trebuie efectuată DPIA? - Anterior prelucrării și pe tot parcursul ciclului de viață al procesului.

Studiul de impact trebuie realizat din momentul conceperii procesului de prelucrare „anterior prelucrării" (art. 35 (1) și art. 35 (1), aspecte ce se regasesc și la considerentele 90 si 93.

Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit (art. 25 relevat și la considerentul 78).

Monitorizarea DPIA pe parcursul ciclului de viață va asigura protecția datelor si a vieții private și va stimula organizația să adopte măsuri care vor proteja efectiv drepturile și libertățile persoanelor vizate.

DPIA este un proces în desfășurare, vizează procesele dinamice și care sunt supuse în mod continuu schimbărilor ce pot crea un risc ridicat în procesarea datelor.

Operatorul este responsabil pentru realizarea unei DPIA(art. 35 (2)).

Operatorul ramâne în cele din urmă responsabil pentru realizarea unui DPIA, chiar dacă studiul poate fi efectuat și de către altcineva din interiorul sau exteriorul organizației.

Operatorul solicită avizul responsabilului cu protecția datelor (DPO), - art. 35 (2).Avizul responsabilului trebuie specificat în studiul de impact. DPO trebuie să monitorizeze funcționarea DPIA - art. 39 (1) lit (c).

Dacă prelucrarea este efectuată de persoana împuternicită de operator, persoana împuternicită de operator va oferi suportul operatorului cu scopul de a pune în practică acele măsuri necesare să protejeze drepturile și libertățile persoanelor vizate, cf. cu art. 28 (3) litera f).

RGPD stabileste caracteristicile minime ale unei DPIA (art. 35 (7) și Considerentele 84 si 90):

- „o descriere a operațiunilor de prelucrare preconizate și scopurilor prelucrării”;
- „o evaluare a necesității și proporționalității prelucrării”;
- „o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate”;
- „măsurile preconizate în vederea abordării riscurilor și a demonstrării conformității cu dispozițiile prezentului Regulament”.

Implementarea DPIA este scalabilă.

Scalabilitatea este proprietatea unui sistem, sau a unui proces, care indică capacitatea de a suporta corect o variație pozitivă a datelor prelucrate, un volum crescut de încarcare.

Scalabilitatea permite suportarea sistemului de a prelucra acele fluxuri mărite de date = suprasolicitare la variații.

Este un element pentru diminuarea riscurilui unui sistem.

Consultarea prealabilă la efectuarea unui DPIA

Ar trebui consultate toate părțile interesate interne relevante, actorii importanți din cadrul organizației de care depinde întreg procesul de prelucrare, supraveghere și monitorizare a activității identificate și în special oricine are responsabilitatea securității informațiilor.

De asemenea, se recomandă ca organizația să ia în considerare solicitarea de consiliere juridică sau consiliere de la alți experți independenți, cum ar fi experți IT, sociologi sau eticieni, după caz.

Cu toate acestea, nu există cerințe specifice pentru a face acest lucru. Răspunderea rămâne în continuare a conducerii organizației, care răspunde de măsurile tehnico organizatorice adoptate, precum și de efectuarea unui DPIA.

Publicarea unei DPIA, nu este o cerință obligatorie, este doar decizia operatorului de a face acest lucru, dar publicarea unui rezumat sau a concluziilor DPIA, oferă încredere în capacitatea organizației de a proteja datele prelucrate.

Este o practica deosebit de buna de a publica o DPIA atunci când membrii publicului sunt afectați de operațiunea de prelucrare.

Atunci când un studiu de impact dezvăluie riscuri reziduale ridicate, va trebui să se solicite consultări prealabile de la autoritatea de supraveghere - art. 36 (1).

Autoritatea de supraveghere poate să furnizeze opinia sa și nu va compromite secretele comerciale sau nu va dezvălui vulnerabilitățile privind securitatea, sub rezerva principiilor aplicabile în fiecare stat membru privind accesul public la documentele oficiale.

Studiul de impact este o parte esențială a conformării cerințelor Regulamentului, atunci când este inițiată o activitate de prelucrare a datelor cu caracter personal cu risc ridicat, sau care există deja.

În cazul în care este planificată o prelucrare cu risc ridicat, operatorul de date trebuie:

1. Să aleagă o metodologie DPIA
2. Să consulte autoritatea de supraveghere atunci când riscul rezidual este mare;
3. Să revizuiască DPIA și activitatea.
4. Să documenteze deciziile luate.
5. Să demonstreze măsurile adoptate.

Pseudonimizarea, limitarea, criptarea datelor cu caracter personal" nu sunt măsuri suficiente, sunt exemple.

Măsurile corespunzatoare depind de context și riscuri, specifice operațiunilor de prelucrare.

Măsuri care contribuie la proporționalitatea și necesitatea prelucrării pe baza:

1. scopurilor determinate, explicite și legitime (art. 5 (1) b));
2. legalitatea prelucrării (art. 6);
3. adecvate, relevante și limitate la ceea ce este necesar (art. 5 (1) c));
4. perioadă de stocare limitată (art. 5 (1) e));

Măsuri care contribuie la drepturile persoanelor vizate:

a) informațiile furnizate persoanei vizate (art. 12, 13 si 14);

b) dreptul de acces și dreptul la portabilitatea datelor (art. 15 si 20);
c) dreptul la rectificare și dreptul la ștergere (art. 16, 17 si 19);
d) dreptul la opoziție, dreptul la restricționarea prelucrării (art. 18, 19, 21);
e) relațiile cu persoanele împuternicite de operator (art. 28);
f) garanțiile pentru transferurile internaționale (Capitolul V);
g) consultarea prealabilă (art. 36).

Atunci când operatorul consideră că o activitate nu este „susceptibilă de a genera un risc ridicat", trebuie să:

1. Să justifice și să documenteze motivele pentru care nu a realizat o DPIA.
2. Evaluarea riscului trebuie să existe.
3. Opinia responsabilului pentru protecția datelor să existe la documentație.
4. Va păstra evidența activităților de prelucrare desfașurate sub responsabilitatea sa, menționate la art. 32 (1) și impuse de securitatea prelucrării datelor specificate la (art. 30 (1)).
5. Monitorizarea continuă a activității.
6. Măsuri de răspuns în cazul unui incident.

Când este necesară efectuarea DPIA?

Când prelucrarea de date care este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice

Evaluarea DPIA conține cel puțin:

1. o descriere sistematică a operațiunilor de prelucrare și a scopurilor prelucrării;
2. o evaluare a necesității și proporționalității operațiunilor raportate la scopuri;
3. o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate;
4. măsurile abordate pentru reducerea riscurilor, măsurile de securitate menite să asigure protecția datelor cu caracter personal.

De ce trebuie să ținem cont?

1. Implementarea DPIA este scalabilă.
2. DPIA reprezintă un proces pentru construirea și demonstrarea conformității.
3. Consultarea Autorității când DPIA dezvăluie riscuri reziduale ridicate, operatorul de date va trebui să solicite consultări pentru prelucrare de la Autoritate.
4. Operatorii nu pot scăpa de răspunderea lor prin acoperirea riscurilor prin polițele de asigurare.

Articolul 25

Asigurarea protecției datelor începand cu momentul conceperii și în mod implicit

(1)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.

(2) Operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării.

Respectiva obligație se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor. În special, astfel de măsuri asigură că, în mod implicit, datele cu caracter personal nu pot fi accesate, fără intervenția persoanei, de un număr nelimitat de persoane.

Pentru asigurarea protecției datelor începand cu momentul conceperii și în mod implicit se vor folosi câteva metode pentru securizarea prelucrării datelor:

1. Consultarea specialiștilor din momentul conceperii procesului.
2. Limitarea numărului de persoane care au acces la date.
3. Pseudominizarea este o tehnică care reduce și mai mult numărul de persoane care au acces la identificarea persoanelor vizate.
4. Limitarea datelor colectate raportate la scopul prelucrării și temeiului legal.
5. Stabilirea unor metode automate de salvare și restaurare a datelor prelucrate dar și a sistemelor informatice în caz de incidente.
6. Stabilirea unor responsabili de procese.

Articolul 32 Securitatea prelucrării

(1)Având în vedere stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul și persoana împuternicită de acesta implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:

a) pseudonimizarea și criptarea datelor cu caracter personal;
b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;

(2)La evaluarea nivelului adecvat de securitate, se ține seama în special de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

(3)Operatorul și persoana împuternicită de acesta iau măsuri pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator și care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care această obligație îi revine în temeiul dreptului Uniunii sau al dreptului intern.

Repere importante de reținut:

1. Securitatea prelucrării
2. Metode folosite pentru a asigura securitatea prelucrării:
3. Criptarea, Pseudonimizarea.
4. Asigurarea confidențialității.
5. Integritatea, disponibilitatea și rezistența continuă a datelor.
6. Capacitatea de a restabili disponibilitatea datelor.
7. Proces pentru testarea, evaluarea și aprecierea periodică.
8. Limitarea accesului uman și a datelor necesare.
9. Moduri care conduc la compromiterea siguranței datelor:
10. Distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la date în mod accidental sau ilegal.

Articolul 46

Transferuri în baza unor garanții adecvate

(1)În absența unei decizii în temeiul articolului 45 alineatul (3), operatorul sau persoana împuternicită de operator poate transfera date cu caracter personal către o țară terță sau o organizație internațională numai dacă operatorul sau persoana împuternicită de operator a oferit garanții adecvate și cu condiția să existe drepturi opozabile și căi de atac eficiente pentru persoanele vizate.

Garanțiile adecvate menționate la alineatul 1 pot fi furnizate fără să fie nevoie de nicio autorizație specifică din partea unei autorități de supraveghere, prin:

a. un instrument obligatoriu din punct de vedere juridic și executoriu între autoritățile sau organismele publice;
b. reguli corporatiste obligatorii în conformitate cu articolul 47;
c. clauze standard de protecție a datelor adoptate de Comisie în conformitate cu procedura de examinare menționată la articolul 93 alineatul (2);
d. clauze standard de protecție a datelor adoptate de o autoritate de supraveghere

CAPITOLUL V. MĂSURI/INSTRUMENTE/PROCEDURI APLICABILE LA NIVEL NAŢIONAL ŞI EUROPEAN ŞI INTERDEPENDENȚA LOR ÎN DOMENIUL SPECIFIC FESI

Concomitent cu intrarea în vigoare a Regulamentului UE nr. 679/2016 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 (Regulamentul UE) activitatea de prelucrare a datelor cu caracter personal este *reglementată unitar la nivelul Uniunii Europene*.

La nivel național, în temeiul prevederilor Regulamentului UE, a fost adoptată Legea nr. 190 din 18 iulie 2018 (denumită în continuare legea națională), al carei obiect este delimitat de puterea legiuitoare română prin dispozițiile art. 1, potrivit cărora „prezenta lege stabilește măsurile necesare punerii în aplicare la nivel național, în principal, a prevederilor art. 6 alin. (2), art. 9 alin. (4), art. 37-39, 42, 43, art. 83 alin. (7), art. 85 și ale art. 87-89 din Regulamentul (UE) 2016/679...” Tot la nivel național, Autoritatea de supraveghere (ANSPDCP) a publicat mai multe decizii cu caracter normativ pe aspecte de interes cum ar fi:

- Decizia nr. 133/3 iulie 2018 privind aprobarea Procedurii de primire şi soluționare a plângerilor
- Decizia nr. 238/18 decembrie 2019 privind modificarea anexei nr. 2 la Procedura de efectuare a investigațiilor
- Decizia nr. 174/18 octombrie 2018 privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal.

Măsuri și instrumente de implementare, monitorizare și control a prelucrării datelor cu caracter personal

Articolul 24 din Regulamentul UE stabilește în mod expres responsabilitatea operatorului în aplicarea de măsuri tehnice și organizatorice. Astfel, ținând seama de natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi de riscurile cu grade diferite de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice, operatorul pune în aplicare măsuri tehnice şi organizatorice adecvate pentru a garanta şi a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu Regulamentul UE. Respectivele măsuri se revizuiesc şi se actualizează dacă este necesar. Atunci când sunt proporționale în raport cu operațiunile de prelucrare aceste măsuri includ punerea în aplicare de către operator a unor politici adecvate de protecţie a datelor. Aderarea la coduri de conduită aprobate, menționate la articolul 40, sau la un mecanism de certificare aprobat, menționat la articolul 42, poate fi utilizată ca element care să demonstreze respectarea obligațiilor de către operator.

Măsurile necesare pentru asigurarea drepturilor persoanelor fizice și a securității prelucrării datelor cu caracter personal includ:

1. Stabilirea persoanelor autorizate să prelucreze date cu caracter personal
2. Asigurarea respectării drepturilor persoanelor fizice

3. Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit (art.25).
4. Organizarea securității și confidentialității prelucrărilor
5. Asigurarea și gestionarea de măsuri de securitate adecvate
6. Asigurarea realizării evaluării impactului asupra protecției datelor
7. Asigurarea evaluării riscului prelucrării asupra drepturilor persoanelor vizate
8. Stabilirea instrucțiunilor documentate de prelucrare pentru împuterniciți
9. Desemnarea responsabilului cu protecția datelor obligatoriu, în condițiile legii
10. Măsuri de prevenire și combatere a faptelor de corupție
11. Măsuri de organizare a unui sistem de control

Vom analiza în cele ce urmează aspectele relevante privind măsurile necesare pentru a se asigura securitatea prelucrării și protejarea drepturilor persoanelor vizate în ceea ce privește prelucrarea datelor cu caracter personal.

1. Stabilirea persoanelor autorizate să prelucreze date cu caracter personal

Operatorul trebuie să stabilească persoanele cu atribuții în prelucrarea datelor cu caracter personal prin fișa postului, prin regulamente ori prin decizii/ordine interne. În baza prevederilor art. 29 din Regulamentul UE, persoana împuternicită de operator şi orice persoană care acţionează sub autoritatea operatorului sau a persoanei împuternicite de operator care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care dreptul Uniunii sau dreptul intern îl obligă să facă acest lucru.

2. Asigurarea respectării drepturilor persoanelor fizice

Nerespectarea oricărui drept prevăzut de dispozițiile Regulamentului atrage răspunderea operatorului. De aceea, operatorii organizează adecvat asigurarea drepturilor persoanelor vizate prin mecanisme de soluționare a cererilor primite, prin numirea unui responsabil cu protecția datelor, prin organizarea de instruiri periodice cu personalul și prin efectuarea de audituri specifice pe protecția datelor.

Măsurile concrete de respectare a drepturilor persoanelor fizice sunt organizate sub forma unei proceduri sau instrucțiuni interne și se referă la circuitul cererilor adresate de petiționari în legătură cu drepturile speciale prevăzute de Regulamentul UE, conținutul și comunicarea răspunsului în termen legal. Se vor pune la dispoziția persoanelor fizice informări redactate într-un limbaj simplu, astfel încât acestea să poată înțelege modul în care sunt utilizate datele lor personale și dacă sunt respectate prevederile legale în domeniu.

3. Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit (art.25).

Operatorul este responsabil și de asigurarea protecției datelor începând cu momentul conceperii și în mod implicit (art.25). Acesta, atât în momentul stabilirii mijloacelor de prelucrare, cât şi în cel al prelucrării în sine, pune în aplicare măsuri tehnice şi organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate să pună în aplicare în mod eficient principiile de protecţie a datelor, precum reducerea la minimum a datelor, şi să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerinţele prezentului regulament şi a proteja drepturile persoanelor vizate.

Potrivit prevederilor art. 4 pct. 5 din Regulamentul UE "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 şi să facă obiectul unor măsuri de natură tehnică şi organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile.

Operatorul pune în aplicare măsuri tehnice şi organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării. Respectiva obligaţie se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare şi accesibilităţii lor. În special, astfel de măsuri asigură că, în mod implicit, datele cu caracter personal nu pot fi accesate, fără intervenţia persoanei, de un număr nelimitat de persoane. Un mecanism de certificare aprobat în conformitate cu articolul 42 poate fi utilizat drept element care să demonstreze îndeplinirea cerinţelor prevăzute de art. 25

4. Organizarea securității și confidențialității prelucrărilor

La nivelul unei organizații se va proceda la definirea unei structuri funcționale de tehnologia informației, luând în considerare cerințele cu privire la personal, abilități, funcții, responsabilități, autoritate, roluri și supraveghere. Structura funcțională este inclusă într-un cadru de referință al procesului de tehnologia informației care asigură transparența și controlul, precum și implicarea atât la nivel executiv cât și general.

Asigurarea securității sistemelor informaționale publice și private se realizează prin securitatea locului de amplasare, securitatea echipamentelor (asigurarea echipamentelor împotriva intențiilor de modificare a lor, controlul integrității echipamentelor, proceduri de întreținere a echipamentelor, toleranța la cădere a echipamentelor, contractele), Securitatea software (obiectivele securității prin software, limitele softului pentru asigurarea securității, măsurile generale de asigurare a securității softului), securitatea personalului (responsabilități manageriale pe linia personalului, măsuri pe linia securității din punct de vedere al personalului), securitatea la nivelul întregului sistem informatic (izolarea sistemelor informatice, controlul accesului sistemelor informatice, detecția amenințărilor și supravegherea sistemului prin urmărirea amenințărilor, etc.), măsuri administrative pe linia securității sistemelor (Securitatea sectorului public, Securitatea sistemelor informaționale din domeniul privat prin obligațiile contabilului șef, obligațiile secretariatului și oficiului juridic, rolul vicepreședintelui cu probleme administrative, organizarea securității firmelor), responsabilități intra organizaționale pe linia prelucrării automate a datelor (prin responsabilitățile directorului sistemului de prelucrare automată a datelor, obligațiile responsabilului cu securitatea, controlul accesului la elementele patrimoniale, urmărirea respectării măsurilor de securitate, principii administrative privind responsabilitățile de securitate).

Reiterăm faptul că, atât operatorul cât şi împuternicitul trebuie să ia măsuri de securitate. Anterior intrării în vigoare a GDPR erau aplicabile prevederile Ordinului Avocatului Poporului nr. 52/2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal, în scopul protejării datelor personale împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, în special dacă prelucrarea respectivă comportă transmisii de date în cadrul unei reţele, precum şi împotriva oricărei alte forme de prelucrare ilegală. Desi acest ordin și-a încetat aplicabilitatea prin dispoziția autoritatii de supraveghere adoptată la data

intrării în vigoare a GDPR, apreciem totuși că prevederile sale pot fi luate în continuare în considerare, cu caracter de recomandare cu privire la:

a) Identificarea şi autentificarea utilizatorului
b) Tipul de acces
c) Colectarea datelor
d) Copiile de siguranţă
e) Computerele şi terminalele de acces
f) Fişierele de acces
g) Sistemele de telecomunicaţii
h) Instruirea personalului
i) Folosirea computerelor
j) Imprimarea datelor

5. Asigurarea și gestionarea măsurilor de securitate adecvate

Potrivit prevederilor art. 32 alin. 1 din GDPR, operatorul și persoana imputernicită de acesta implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzator riscurilor identificate, incluzând printre altele, după caz:

a) pseudonimizarea și criptarea datelor cu caracter personal;
b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;
c) capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
d) un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

Subliniem faptul că, încălcarea securității datelor este o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea. În acest scop, operatorul ia măsuri de stabilire a unei echipe de gestionare a incidentelor de securitate, ca structură locală, cu atribuții în identificarea, înregistrarea, raportarea și rezolvarea oricărui incident de securitate. Această echipa poate fi formată din unul sau mai multi specialiști (după caz) din compartimentele: juridic, IT, resurse umane și alte specializări tehnice (unde este cazul). Echipa va fi condusă de Responsabilul cu protecția datelor. Cum se clasifică o încălcare a securității datelor cu caracter personal:

- Incălcare privind confidențialitatea – atunci când există o divulgare accidentală sau neautorizată a datelor cu caracter personal sau un acces neautorizat la acestea;
- Incălcare privind disponibilitatea – atunci când datele sunt pierdute în mod accidental sau ca urmare a unor activități neautorizate sau când aceste date sunt distruse
- Incălcare privind integritatea – atunci când datele suferă modificari în mod accidental sau ca urmare a unor activități neautorizate

Operatorul informează de îndată persoanele vizate cu privire la încălcarea securității datelor, în temeiul art. 34 din Regulament.

Operatorul păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse. Această documentație permite autorității de supraveghere să verifice conformitatea cu Regulamentul.

6. Asigurarea realizării evaluării impactului asupra protecției datelor

O altă obligație ce incumbă operatorului se referă la evaluarea impactului prelucrării asupra drepturilor persoanelor vizate. Evaluarea impactului asupra protecției datelor este obligatorie, potrivit reglementării art. 35:

a. în cazuri de risc ridicat, prealabil începerii preucrărilor de date personale
b. în caz de prelucrare automată, inclusiv creare de profiluri,
c. prelucrare pe scară largă a datelor speciale si monitorizarea pe scară largă a unei zone accesibile publicului
d. conținut minim: descrierea operațiunilor și a scopului prelucrării, evaluarea necesității și proporționalității operațiunilor pe scop de prelucrare, măsurile de atenuare a riscurilor și de securitate, inclusiv garanțiile (mecanismele menite să asigure drepturile și interesele persoanelor vizate)

Această evaluare se face în considerarea naturii, domeniului de aplicare, contextului și scopurilor prelucrării în cazurile în care un tip de prelucrare (în special ce bazat pe utilizarea noilor tehnologii) este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile unei persoane fizice.

Atunci când prelucrarea în temeiul articolului 6 alineatul (1) litera (c) sau (e) 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 şi deja s-a efectuat o evaluare a impactului asupra protecției datelor ca parte a unei evaluări a impactului general în contextul adoptării respectivului temei juridic, alineatele (1)-(7) ale art. 35 nu se aplică, cu excepția cazului în care statele membre consideră că este necesară efectuarea unei astfel de evaluări înaintea desfăşurării activităţilor de prelucrare. Subiectul va fi detaliat pe parcursul suportului de curs.

7. Asigurarea evaluării riscului prelucrării asupra drepturilor persoanelor vizate

Sub aspectul identificării și evaluării riscului, măsurile întreprinse de operator urmăresc diminuarea probabilității (posibilității) de aparitie a riscului, dar și diminuarea consecințelor (impactului) asupra rezultatelor (obiectivelor) în situația în care riscul se materializează.

Evaluarea riscului înseamna evaluarea consecinţelor (impactului) materializării riscului, în combinaţie cu evaluarea probabilităţii, în raport cu obiectivele prestabilite, în cazul în care riscul se materializează. Evaluarea riscului reprezintă evaluarea expunerii la risc. Subiectul va fi detaliat pe parcursul suportului de curs.

8. Stabilirea instrucțiunilor documentate de prelucrare pentru imputerniciți

Relaţia dintre operator şi persoanele împuternicite care prelucrează date cu caracter personal pe seama operatorului se realizează pe baza încheierii unor contracte în formă scrisă.

Prin contract se stabilesc următoarele: obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal, categoriile de persoane vizate, obligațiile și drepturile operatorului. Cele două entități juridice semnatare ale contractului cooperează în cazul unor breșe de securitate, situație în care trebuie să prevadă în mod expres în contract obligațiile ce le revin în asigurarea notificării ANSPDCP înlăuntrul termenului de 72 de ore prevazut de GDPR.

Respectivul contract sau act juridic prevede în special că persoana împuternicită de operator:

a) prelucrează datele cu caracter personal numai pe baza unor instrucţiuni documentate din partea operatorului, inclusiv în ceea ce priveşte transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, cu excepția cazului în care această obligaţie îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică; în acest caz, notifică această obligaţie juridică operatorului înainte de prelucrare, cu excepția cazului în care dreptul respectiv interzice o astfel de notificare din motive importante legate de interesul public;
b) se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidenţialitatea sau au o obligaţie statutară adecvată de confidenţialitate;
c) adoptă toate măsurile necesare în conformitate cu articolul 32;
d) respectă condițiile menționate la alineatele (2) şi (4) privind recrutarea unei alte persoane împuternicite de operator;
e) ţinând seama de natura prelucrării, oferă asistenţă operatorului prin măsuri tehnice şi organizatorice adecvate, în măsura în care acest lucru este posibil, pentru îndeplinirea obligației operatorului de a răspunde cererilor privind exercitarea de către persoana vizată a drepturilor prevăzute în capitolul III;
f) ajută operatorul să asigure respectarea obligaţiilor prevăzute la articolele 32-36, ţinând seama de caracterul prelucrării şi informațiile aflate la dispoziția persoanei împuternicite de operator;
g) la alegerea operatorului, şterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare şi elimină copiile existente, cu excepția cazului în care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal;
h) pune la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea obligaţiilor prevăzute la prezentul articol, permite desfăşurarea auditurilor, inclusiv a inspecţiilor, efectuate de operator sau alt auditor mandatat și contribuie la acestea.

9. Desemnarea responsabilului cu protecția datelor obligatoriu, în condițiile legii

Numirea unui Responsabil cu protecția datelor constituie o obligație legală pentru autoritățile și instituțiile publice, o garanție de conformitate pentru toți operatorii de date personale și împuterniciții acestora.

Potrivit prevederilor art. 10 din Legea nr. 190/2018 operatorii şi persoanele împuternicite de operator desemnează un responsabil cu protecția datelor în situațiile şi condițiile prevăzute la art. 37-39 din Regulamentul general privind protecția datelor.

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

Activitatea şi sarcinile responsabilului cu protecția datelor se realizează cu respectarea prevederilor art. 38 şi 39 din Regulamentul general privind protecția datelor şi a reglementărilor legale naţionale aplicabile. Subiectul va fi detaliat pe parcursul suportului de curs.

10. Măsuri de prevenire și combatere a faptelor de corupție

Operațiunile de prelucrare a datelor cu caracter personal vizează atât circuitul documentelor pe suport de hârtie cât și prelucrarea informațiilor prin sistem informațional în sens larg, ori prin aplicații specifice de monitorizare și control.

Cu privire la fluxul documentelor pe suport de hârtie ce includ date cu caracter personal operatorul va stabili responsabilități clare de acces, verificare și control al acestora. În mod obișnuit se întocmește o procedură operațională de lucru pentru această categorie de documente, se clasifică natura datelor cuprinse și se identifică regimul și traseul documentelor, cu respectarea principiilor art. 5 din Regulamentul UE.

Cu privire la datele prelucrate automat în sistem informatic, prin aplicație, se iau măsuri tehnice adecvate de protecție a echipamentului, securitate a softului, a accesului controlat la aplicație și sistem, documentarea procedurilor de operare, stabilirea corectă a cerințelor de acordare a drepturilor de utilizare a datelor, precum și integrarea prevederilor art. 25 în arhitectura sistemului informatic/aplicației.

Sistemele informatice sunt amenințate atât din interior cât şi din exterior. Pot fi persoane bine intenționate care fac diferite erori de operare sau persoane rău intenționate, care sacrifică timp şi bani pentru penetrarea sistemelor informatice. Oamenii care administrează sistemul sau doar folosesc calculatorul reprezintă cea mai mare vulnerabilitate pentru securitatea acestuia.

ISO/IEC 27001 este principalul standard pentru managementul securității informației ce acoperă organizații (comerciale, guvernamentale, non-profit), stabilește cerințele pentru un Sistem de Management al Securității Informației (SMSI) și ajută la identificarea, managementul și minimizarea amenintarilor care afectează de obicei informația.

Separarea responsabilităților este unul din cele mai importante aspecte ale securității unui sistem, indiferent dacă este vorba despre securitatea unui întreg sistem sau doar a unei singure component, de exemplu, modul de acces la sistemul de baze de date din organizație.

Separarea atribuțiilor este o direcție de evaluare a cadrului organizatoric prin *care se evită un conflict al sarcinilor în sensul că nicio persoană nu are responsabilități sau un*

acces care să îi permită acesteia să abuzeze sau să redirecţioneze activele societăţii fără a fi descurajată sau detectată în timp util. Sub acest aspect putem face referire la mai multe aspecte relevante:

- Includerea cu claritate a atribuțiilor personalului în fișa postului, în scopul reducerii riscului efectuării de către acesta a unor acțiuni dincolo de limitele autorizate;
- Separarea sarcinilor realizată prin intermediul sistemului informatic, prin utilizarea de profile de securitate individuale și de grup, preprogramate;
- Existența unei separări fizice și manageriale a atribuțiilor, pentru a reduce riscul de fraudă;
- Separarea sarcinilor în cadrul compartimentului IT pe categorii de activități
- Separarea sarcinilor administratorului de sistem de cele de control al securității sistemului
- Interdicția ca programatorii să aibă acces la introducerea de date, fișiere permanente cu date de ieșire, programe, etc. pentru a-și îndeplini sarcinile

Utilizatorii obişnuiţi, operatorii, programatorii sau oamenii care întreţin sistemul pot fi corupţi sau forţaţi să divulge parole, informaţii sau căi de acces, cu alte cuvinte să compromită securitatea computerelor. Securizarea se poate pune în aplicare prin diverse metode pornind de la încuierea încăperilor cu calculatoare şi a calculatorului însuşi, protejarea intrărilor în reţeaua de calculatoare cu parole, folosirea sistemelor de protejare a fişierelor de date pentru împiedicarea distrugerii acestora, criptarea liniilor de comunicaţii din reţelele de calculatoare şi ajunge până la folosirea unor tehnologii speciale pentru împiedicarea interceptării diferitelor radiaţii emise de echipamentele de calcul în timpul funcţionarii normale a acestora.

Măsurile de prevenire și combatere a faptelor de combatere a corupției vizează persoanele care au acces la sistemul informatic, astfel încât, sub acest aspect, un rol important îl ocupă seriozitatea și competența personalului în respectarea procedurilor operaționale, în exercitarea corectă a verificării operațiunilor de prelucrare și în efectuarea la anumite intervale de timp a unor audituri de specialitate. Un rol important în activitatea de verificare îl are și Responsabilul cu protecția datelor cu caracter personal.

11. Măsuri de organizare a unui sistem de *control*

În conformitate cu prevederile Ordinului nr. 600/2018 emis de secretarul general al Guvernului cu privire la aprobarea Codului controlului intern managerial al entităților publice, ”Conducătorul fiecărei entități publice dispune... măsuri necesare pentru implementarea și dezvoltarea sistemului de control intern managerial.” (art. 2)

În temeiul prevederilor art. 39 alin. 1 lit.b din Regulamentul UE, Responsabilul cu protecția datelor are sarcina legală de monitorizare a respectării prevederilor regulamentului, a altor dispoziții de drept al Uniunii sau de drept intern referitoare la protecția datelor şi a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce priveşte protecția datelor cu caracter personal, inclusiv alocarea responsabilităţilor şi acţiunile de sensibilizare şi de formare a personalului implicat în operațiunile de prelucrare, precum şi auditurile aferente. În acest sens, conducătorul poate aproba Responsabilului cu protecția datelor un Plan de activitate de verificare și/sau control al operațiunilor de prelucrare a datelor cu caracter personal. De asemenea,

pot fi efectuate și verificări ad-hoc ale prelucrărilor efectuate de un utilizator ori structură a entității, dacă se bănuiește ori se reclamă existența unei vulnerabilități.

Dincolo de controlul managerial intern ori cel efectuat de Responsabilul cu protecția datelor, entitățile publice sunt auditate de Curtea de conturi a României.

Nu în ultimul rând trebuie să amintim activitatea de control pe care o exercită Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal asupra conformității prelucrării datelor cu caracter personal cu prevederile Regulamentului UE și a legislației naționale în domeniu.

Instrumentele care asigură implementarea măsurilor luate de operator cu privire la confidențialitatea, integritatea și disponibilitatea datelor cu caracter personal în timpul prelucrării.

Operatorul de date cu caracter personal are posibilitatea să includă măsurile tehnice și cele organizatorice de protejare a drepturilor persoanelor vizate în regulamente specifice, în instrucțiuni, în proceduri și politici specifice de prelucrare a datelor cu caracter personal. Este corectă și includerea măsurilor adoptate pentru asigurarea conformității operațiunilor de prelucrare în procedurile deja existente privind securitatea și confidențialitatea sistemelor informatice, controlul managerial intern, managementul performanței, managementul calității, managementul riscului, etc. Dacă se optează pentru această din urmă variantă, trebuie ca operatorul să asigure punerea la dispoziția Autorității naționale de supraveghere, la cererea acesteia, a tuturor documentelor referitoare la implementarea dispozițiilor Regulamentului UE nr. 679/2016. De la caz la caz, operatorii din sectorul public ce se înscriu în domeniul de reglementare al Legii nr. 190/2018, trebuie să asigure punerea în aplicare a prevederilor acestui act normativ. Subliniem faptul că, există sectoare de activitate reglementate specific prin ordonanțe, hotărâri de guvern, ordine, norme metodologice și instrucțiuni ce cuprind referiri la prelucrarea datelor cu caracter personal aplicabile în domeniile respective.

Relația instituțională cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) se desfășoară, în condițiile legii, prin instrumente specifice, cum ar fi notificarea breșelor de securitate, prin cereri de consultare prealabilă ori de obținere a aprobărilor legale din partea acesteia. De regulă, deciziile cu caracter normativ adoptate și publicate de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal oferă orientări și clarificări importante în luarea măsurilor de către operatori în domeniul prelucrării datelor cu caracter personal, în acord cu orientările, recomandările și bunele practici adoptate și publicate de Comitetul european pentru protecția datelor.

Constituie instrumente de implementare:

- **a.** Politicile interne referitoare la securitatea și confidențialitatea prelucrării datelor
- **b.** Notificarea Autorității de supraveghere în cazul încălcării securității datelor
- **c.** Evaluarea impactului asupra protecției datelor
- **d.** Consultarea prealabilă a Autorității de supraveghere în cazul identificării unor riscuri mari în activitatea de prelucrare.
- **e.** Verificări ad-hoc prin acțiuni concrete de verificare a modului în care sunt implementate măsurile tehnice și organizatorice specifice de asigurare a securității prelucrării datelor cu caracter personal

f. Auditarea securității și confidențialității prelucrărilor de date cu caracter personal
g. Instruirea periodică a personalului implicat în prelucrarea datelor cu caracter personal

Vom analiza în cele ce urmează aspectele relevante privind instrumentele necesare pentru a se asigura securitatea prelucrării și protejarea drepturilor persoanelor vizate în ceea ce privește prelucrarea datelor cu caracter personal.

a. Politicile interne de securitate și confidențialitate a prelucrării datelor

Politicile cuprind deciziile luate de operator pentru asigurarea cerințelor și măsurilor necesare prelucrării datelor cu caracter personal la nivelul organizației. Politicile se implementează prin acțiuni ale structurilor din subordine, de regulă, cu ajutorul unui program și/sau a unei proceduri, precum și prin organizarea unui sistem de control.

Prin politica internă se va menționa în mod expres faptul că prelucrarea datelor cu caracter personal în sistem informatic se face de personalul anume desemnat prin fișa postului, pe categorii de lucrări, iar conducătorul organizației stabilește, prin decizie, cu avizul responsabilului cu protecția datelor, autorizarea unor funcționari publici/angajați pentru anumite operațiuni de prelucrare.

Redăm un posibil model de politică internă referitoare la prelucrarea datelor cu caracter personal:

1. Utilizatorii trebuie să se identifice. Identificarea se poate face pe baza unui nume de utilizator unic, astfel niciodată mai mulți utilizatori nu au același nume de utilizator. Un utilizator se poate autentifica prin introducerea unei parole. Parolele sunt confidențiale și sunt schimbate periodic.
2. Utilizatorii accesează numai datele cu caracter personal necesare pentru îndeplinirea atribuțiilor de serviciu. Tipul de acces este stabilit pentru fiecare utilizator în parte în funcție de funcționalitate, respectiv administrare, introducere, prelucrare, salvare, precum și în funcție de acțiunile aplicate asupra datelor cu caracter personal: scriere, citire, ștergere.
3. Colectarea/prelucrarea și modificarea datelor caracter personal se face de către personal autorizat.
4. Copiile de siguranța (backup-uri) ale bazelor de date cu caracter personal precum și ale programelor folosite pentru prelucrările automatizate se execută zilnic, automat. Acestea sunt păstrate în camere separate de spațiile în care se operează asupra datelor cu caracter personal, iar accesul la acestea este restricționat.
5. Accesul la computere și alte terminale de acces se face doar prin intermediul unui nume de utilizator și a unei parole. Serverele care găzduiesc bazele de date ce conțin date cu caracter personal pot fi accesate doar în mod controlat și se afla în încăperi cu acces restricționat.
6. Orice accesare a bazei de date cu caracter personal este înregistrata într-un fișier de acces (numit log). Orice încercare de acces neautorizat este de asemenea înregistrată. Entitatea păstrează fișierele de acces cel puțin 3 ani, pentru a fi folosite ca probe in cazul unei investigații. Dacă investigațiile se prelungesc, aceste fișiere se vor păstra atât timp cât se consideră necesar.

7. Actualizarea și verificarea funcționalității programelor care prelucrează date cu caracter personal se face, iar tipul de acces al utilizatorilor este stabilit de userul " ADMIN ".
8. Utilizatorii care au acces la datele cu caracter personal sunt instruiți cu privire la dispozițiile legale in vigoare, la cerințele minime de securitate a prelucrărilor de date cu caracter personal, la riscurile pe care le comporta prelucrarea datelor cu caracter personal, precum și la confidențialitatea asupra acestora. Utilizatorii sunt obligaţi să îşi închidă sesiunea de lucru atunci când părăsesc locul de muncă.
9. Scoaterea la imprimantă a datelor cu caracter personal se realizează numai de utilizatori autorizați pentru aceasta operațiune și numai în cazul în care aceasta va fi strict necesară, documentele imprimate fiind catalogate drept documente confidențiale de uz intern.
10. Conceptul de reproducere se referă la copierea, tipărirea documentelor pe hârtie, copierea fişierelor, a înregistrărilor audio, fotografice sau video şi orice alte mijloace de multiplicare a informaţiei. Operatorii sunt obligaţi să aprobe proceduri interne specifice privind folosirea şi distrugerea acestor materiale. Toate copiile trebuie controlate şi protejate conform acestei politici. În cazul în care utilizarea documentelor imprimate care conţin date personale nu mai este necesară, persoanele care le-au utilizat vor proceda la distrugerea acestora.

b. Notificarea Autorității de supraveghere în cazul încălcării securității datelor personale

Obligația de notificare a breșelor de securitate către Autoritatea de supraveghere va fi detaliată în cadrul procedurii referitoare la încălcarea securității datelor cu caracter personal. Constituirea unui grup de lucru la nivelul operatorului în vederea analizei și soluționării unui incident de securitate, sub coordonarea Responsabilului cu protecția datelor, este de asemenea un instrument eficace de monitorizare a respectării măsurilor tehnice și organizatorice adoptate pentru asigurarea securității prelucrării. Încălcarea securității datelor este definită ca o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea. Se constituie la nivelul organizației o echipă de gestionare a incidentelor de securitate (Incident Response Team/Working Grup) care este structura ce se ocupă cu identificarea, înregistrarea, raportarea și rezolvarea oricărui incident de securitate. Această echipa poate fi formata din unul sau mai multi specialiști (după caz) din compartimentele: juridic, IT, resurse umane și alte specializări tehnice (unde este cazul). Echipa va fi condusă de Responsabilul cu protecția datelor.

Conținutul Notificării adresate Autorității de Supraveghere (ANSPDCP) în cazul încălcării securității datelor cu caracter personal se află la dispoziția operatorilor de date pe site-ul official www.dataprotection.ro (formular breșă).

Notificarea în cazul încălcării securității datelor

În temeiul prevederilor art. 33 alin. 1 din Regulament, operatorul notifică ANSPDCP *fără intarzieri nejustificate* și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care este puțin probabil să genereze un risc pentru drepturile și libertățile persoanelor fizice. Atunci când notificarea către autoritatea de supraveghere nu are loc în termen de 72 de ore, aceasta este însoțită de o explicație motivată pentru întârziere.

În situația prelucrărilor efectuate prin împuternicit, acesta înștiințează operatorul, fără întârzieri nejustificate, după ce ia cunoștință de o încalcare a securității datelor cu caracter personal. *Notificarea adresată ANSPDCP trebuie:*

- Să descrie caracterul încălcarii securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;

- Să comunice numele și datele de contact ale responsabilului cu protecția datelor de unde se pot obține mai multe informații;
- Să descrie consecințele probabile ale încălcării securității datelor cu caracter personal;
- Să descrie măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor efecte negative.

Operatorul informează de îndata persoanele vizate cu privire la încălcarea securității datelor, în temeiul art. 34 din Regulament

c. Evaluarea impactului asupra protecției datelor

Evaluarea impactului asupra protecției datelor este un instrument important de responsabilizare deoarece ajută operatorii de date nu numai să respecte cerințele Regulamentului UE nr. 679/2026, ci și să demonstreze că au fost luate măsuri adecvate pentru a asigura conformitatea cu Regulamentul În general,realizarea unei evaluări a impactului aceasta este obligatorie în măsura în care prelucrarea se încadrează în ipotezele reglementate de art. 35 din Regulamentul (UE) 2016/679 coroborat cu Decizia nr. 174/2018 privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal.

În același timp, în Opinia nr. 248/2017 privind Orientări privind evaluarea impactului asupra protecției datelor (DPIA) și modul în care se determină dacă prelucrarea este „susceptibilă să genereze un risc ridicat” în sensul Regulamentului 2016/679, Grupul de Lucru Art. 29 a recomandat următoarele:

”În cazurile în care nu este clar dacă este necesară o DPIA, WP29 recomandă efectuarea, cu toate acestea, a unei DPIA, întrucât o DPIA este un instrument util pentru a sprijini operatorii să respecte legislația în materie de protecție a datelor.”

În măsura în care operatorul nu efectuează o evaluare a impactului, Grupul de Lucru Art. 29 menționează în documentul său că ”În astfel de cazuri, operatorul ar trebui să justifice și să documenteze motivele pentru care nu a efectuat o DPIA și să includă/înregistreze avizele responsabilului cu protecția datelor.”

Având în vedere cele de mai sus, revine operatorului obligația de a analiza în ce măsură prelucrarea respectivă reprezintă un risc ridicat pentru drepturile și libertățile persoanelor vizate, precum și cea de a justifica și documenta motivele pentru care nu a efectuat o astfel de evaluare.

Cu privire la oportunitatea efectutării unei evaluări a impactului prelucrării de către entitățile publice din România, Autoritatea Națională de Supraveghere a Prelucrării

Datelor cu Caracter Personal s-a pronunțat prin Decizia nr. 174 din 18 octombrie 2018 privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal, care a stabilit la art. 1 alineatul 2 următoarele ”Prin excepție de la alin. (1), evaluarea impactului asupra protecției datelor nu este obligatorie atunci când prelucrarea efectuată în temeiul art. 6 alin. (1) lit. (c) sau (e) din Regulamentul general privind protecția datelor are un temei juridic în dreptul Uniunii sau în dreptul intern şi deja s-a efectuat o evaluare a impactului asupra protecției datelor ca parte a unei evaluări generale a impactului în contextul adoptării actelor normative respective”.

d. Consultarea prealabilă a Autorității de supraveghere în cazul identificării unor riscuri ridicate în activitatea de prelucrare.

Operatorul consultă autoritatea de supraveghere înainte de prelucrare atunci când evaluarea impactului asupra protecției datelor indică faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri luate de operator pentru atenuarea riscului. Atunci când consideră că prelucrarea ar încălca regulamentul, în special atunci când riscul nu a fost identificat sau atenuat într-o măsură suficientă de către operator, autoritatea de supraveghere oferă consiliere în scris operatorului şi, după caz, persoanei împuternicite de operator, în cel mult opt săptămâni de la primirea cererii de consultare, şi îşi poate utiliza oricare dintre competențele menționate la articolul 58 din Regulament. Această perioadă poate fi prelungită cu şase săptămâni, ținându-se seama de complexitatea prelucrării prevăzute. Autoritatea de supraveghere informează operatorul în termen de o lună de la primirea cererii, cu privire la orice astfel de prelungire, prezentând motivele întârzierii. Aceste perioade pot fi suspendate până când autoritatea de supraveghere a obținut informațiile pe care le-a solicitat în scopul consultării.

Statele membre consultă autoritatea de supraveghere în cadrul procesului de pregătire a unei propuneri de măsură legislativă care urmează să fie adoptată de un parlament național sau a unei măsuri de reglementare întemeiate pe o astfel de măsură legislativă, care se referă la prelucrare.

Dreptul intern poate impune operatorilor să se consulte cu autoritatea de supraveghere şi să obțină în prealabil autorizarea din partea acesteia în legătură cu prelucrarea de către un operator în vederea îndeplinirii unei sarcini exercitate de acesta în interes public, inclusiv prelucrarea în legătură cu protecția socială şi sănătatea publică.

e. Verificări ad-hoc se efectueaza prin acțiuni concrete de verificare a modului în care sunt implementate măsurile tehnice și organizatorice specifice de asigurare a securității prelucrării datelor cu caracter personal.

Prin regulamente interne, instrucțiuni ori proceduri operatorul prevede activități de verificare a modului cum sunt aduse la îndeplinire măsurile tehnice și cele organizatorice adoptate pentru asigurarea drepturilor persoanelor vizate și a securității operațiunilor de prelucrare a datelor cu caracter personal.

f. Auditarea securității și confidențialității prelucrărilor de date cu caracter personal

Persoanele cu funcții de conducere din organizație trebuie să se asigure că angajații din subordine cunosc şi respectă întotdeauna procedurile de confidențialitate şi securitate a prelucrării datelor. De asemenea, fiecare persoană cu funcție de conducere este direct

răspunzătoare pentru implementarea confidenţialităţii şi securităţii prelucrării datelor prelucrate în cadrul compartimentului său.

Structura unui raport de auditare ar putea cuprinde:

Secţiunea 1. Introducere

1.1. Scopul auditului Paragraful trebuie să prezinte scopul raportului, şi anume prezentarea rezultatelor auditării unui anume produs software sau proiect.

1.2. Identificarea obiectului auditului Paragraful trebuie să conţină identificarea obiectului auditului (produsul sau proiectul auditat), localizarea sa în timp şi spaţiu, perioada când a fost efectuat auditul, numele auditorilor.

1.3. Referinţe despre proiect Paragraful trebuie să conţină un sumar al referinţelor (documentelor şi documentaţiilor) cu privire la istoria şi dezvoltarea proiectului în cadrul căruia a fost executat auditul.

1.4. Sumarul raportului de audit Paragraful trebuie să conţină o scurtă descriere a conţinutului raportului de audit.

Secţiunea 2. Referinţe Această secţiune conţine o listă completă a documentelor pe care se bazează raportul de audit.

Secţiunea 3. Procedura de audit. În această secţiune se va descrie procedura utilizată în conducerea auditului, cu referire la documentele specifice sau alte entităţi utilizate în cadrul procesului.

Secţiunea 4. Constatări

4.1. Conformanţa cu standardele Paragraful trebuie să conţină constatările făcute cu ocazia verificării asigurării calităţii, în ceea ce priveşte structura, formatul, conţinutul şi metodologia. Standardele aplicabile pot fi externe (guvernamentale, internaţionale, departamentale, impuse prin contracte) sau interne (de corporaţie, sau ale managementului de proiect).

4.2. Identificarea configuraţiei Paragraful trebuie să conţină rezultatele identificării configuraţiei software, precum şi o reprezentare grafică a configuraţiei (cuprinsă în paragraf sau într-o anexă la acesta). Tot în acest paragraf vor fi menţionate şi dificultăţile întâmpinate în procesul de deducere a elementelor de configuraţie.

4.3. Rezultatele evaluării cerinţelor Paragraful trebuie să conţină o listă a discrepanţelor observate în evaluarea documentaţiei în care sunt cuprinse cerinţele (specificaţiile cerinţelor). Poate fi cuprinsă la acest paragraf sau într-un apendix şi o reprezentare a cerinţelor identificate. 119 Anexa 3A (continuare)

4.4. Matricea trasabilităţii Paragraful reprezintă trasabilitatea dintre specificaţiile cerinţelor şi produsul software. De asemenea, aici se detaliază discrepanţele dintre

specificațiile cerințelor și produsul software, precum și dintre rezultatele stadiului precedent și produsul software prezent.

4.5. Rezultatele verificării Paragraful trebuie să prezinte discrepanțele observate, ca rezultat al procesului de verificare al produsului software.

4.6. Rezultatele validării Paragraful trebuie să prezinte o listă a discrepanțelor observate, ca rezultat al procesului de validare al produsului software.

4.7. Raportul de stadiu al configurației Paragraful trebuie să conțină o listă a elementelor de configurație care au fost modificate, ca urmare a actualizării produsului software, precum și a modificărilor făcute.

Secțiunea 5. Concluzii Secțiunea prezintă concluziile formulate de auditori, în baza rezultatelor auditului. Aici trebuie să se menționeze că aceste concluzii reprezintă concluziile proprii (și, eventual, subiective) ale autorilor, în comparație, cu rezultatele obiective ale auditului, rezultate din observare și prezentate în secțiunea 4.

Secțiunea 6. Recomandări Secțiunea conține recomandările auditorilor, rezultate în urma auditului. Ca și secțiunea anterioară, și această secțiune conține judecăți și concluzii proprii ale auditorilor (deci se menționează și aici eventuala rezervă de subiectivitate).

g. Instruirea periodică a personalului implicat în prelucrarea datelor cu caracter personal

Multe incidente de securitate sunt generate de personal din interiorul organizației, prin erori ori neglijență în utilizarea resurselor informaționale sau chiar acțiuni rău intenționate. Se tratează riscurile de natură umană ce pot fi induse din interiorul organizației prin măsuri specifice precum includerea responsabilităților legate de securitatea informațiilor în descrierea și sarcinile de serviciu ale postului, implementarea unor politici de verificare a angajaților, încheierea unor acorduri de confidențialitate și prin clauze specifice în contractele de muncă.

Funcționarii publici/angajații trebuie auditati pe întreaga perioadă de valabilitate a contractului de muncă și trebuie să aibă cunoștință de prevederile politicilor de securitate.

Clauzele de confidențialitate, definirea conflictelor de interese, distribuirea și divulgarea informațiilor trebuie avute în vedere pentru fiecare post în parte. Pentru a evita neglijența sau greșelile de operare, utilizatorii ar trebui informați cu privire la amenințările la care sunt supuse informațiile manipulate. Utilizatorii trebuie instruiți cu privire la procedurile de securitate ce trebuie urmate și utilizarea facilităților IT în conformitate cu politica organizației. Ar trebui să existe un program coerent de instruire a angajaților pe diverse niveluri de interes, pe lângă o instruire generală în gestiunea securității fiind necesare și specializări pentru administratorii sistemului informatic în tehnologii de securitate specifice.

Prin urmare, instruirea periodică a personalului implicat în prelucrarea datelor cu caracter personal constituie o măsură necesară pentru orice operator de date cu caracter personal, din sectorul public și privat.

Proceduri aplicabile la nivel naţional şi european şi interdependenţa lor

Politicile interne de securitate și confidențialitate aprobate de operator, pot fi procedurate atât pentru prelucrările de date cu caracter personal pe suport de hârtie, cât și pentru prelucrările realizate în sistem informatic. În acest sens, operatorul are libertate de acțiune, cu respectarea prevederilor art. 5 alin. 2 din Regulament.

Procedurile mai des întâlnite sunt:

Procedura de încălcare a securității datelor personale. Obligația de a elabora procedura de încălcare a securității datelor personale va fi detaliată în cadrul unei proceduri referitoare la încălcarea securității datelor cu caracter personal

Procedura de notificare a breşelor de securitate către Autoritatea de supraveghere poate fi redactată separat ori în cuprinsul procedurii de încălcare a securității datelor.

Procedura de analizare şi evaluare a riscurilor prelucrării cuprinde pașii necesari în identificarea surselor de risc și estimarea riscului, precum și evaluarea acestuia.

Ceea ce este deosebit de important este comunicarea procedurilor persoanelor implicate în prelucrarea datelor cu caracter personal, sub luare de semnătură.

La nivel european, Comisia are competențe clar stabilite în cuprinsul Regulamentului UE, iar deciziile adoptate pe domeniile sale de competență sunt aplicabile statelor membre.

CAPITOLUL VI. RESPECTAREA CERINȚELOR PRIVIND DATELE INFORMATICE ȘI SECURITATEA SISTEMELOR INFORMATICE, INCLUSIV INCIDENȚA ASUPRA FUNCȚIONALITĂȚII MYSMIS

1. Concepte privind securitatea sistemului informațional

1.1 Sistemul informațional

Modelul generic de structurare a unei organizaţii din sfera economică sau adminstrativă cuprinde următoarele subsisteme: subsistemul condus, subsistemul de conducere şi subsistemul informaţional. Fiecare verigă organizatorică desfăşoară pe de o parte o activitate independentă, iar pe de altă parte este interconectată cu celelalte asigurând funcţionarea unitară a întregului sistem, care este coordonat de subsistemul de conducere. Exercitarea funcţiei de conducere la nivelul unei unităţi economice presupune un ciclu decizional compus din mai multe faze definite prin următoarele acţiuni: a prevedea, a organiza, a comanda, a coordona, a controla. Rezultă că informațiile sunt baza procesului decizional exercitat de funcţia de conducere, fluxul de informații fiind cel care asigură legătura între sistemul de conducere şi cel de execuţie. Datorită rolului pe care informațiile îl au la nivelul proceselor logistice şi de conducere, sfera în care acestea se generează şi se utilizează, se conturează distinct ca un sistem independent, şi anume,

sistemul informațional, în cadrul căruia se distinge componenta de prelucrare automată a informațiilor, *sistemul informatic*.

Sistemul informaţional reprezintă un ansamblu interconectat de metode şi tehnici ce contribuie la informarea membrilor unei organizaţii, constituindu-se într-o reţea complexă de informaţii vii şi dinamice, care reprezintă baza proceselor desfăşurate în cadrul organizației. Rezultă că sistemul informaţional are pe de o parte o funcţie de sinteză, oferind o viziune sistemică, globală asupra unei organizaţii, iar pe de altă parte o funcţie de specializare, furnizând informaţii detaliate pentru fiecare categorie de personal. Sistemul informaţional poate fi definit şi ca totalitatea procedurilor organizate care permit furnizarea de informaţii necesare procesului decizional şi funcţiilor de control ale organizației. Sistemul informaţional poate fi privit sub aspect *static* sau *dinamic*. *Aspectul static* al sistemului informaţional presupune înregistrarea în mod structurat a faptelor survenite şi a datelor, consemnându-se regulile şi restricţiile aplicate asupra acestora. *Aspectul dinamic* presupune procesarea informaţiilor, ceea ce implică schimbarea structurilor, regulilor şi restricţiilor ca urmare a evoluţiei în timp a sistemului.

Sistemul informațional se individualizează ca fiind *totalitatea metodelor, tehnicilor şi instrumentelor pentru culegerea, înregistrarea, transmiterea, prelucrarea şi valorificarea informațiilor dintr-o organizație*.

Colectarea, prelucrarea şi transmiterea datelor se efectuează în cadrul unei organizații la nivelul unor verigi organizatorice denumite posturi de lucru. Postul de lucru se caracterizează prin intrările (datele de intrare), ieşirile (datele de ieşire) şi prelucrările efectuate la nivelul respectiv (operaţii de prelucrare şi timp de staţionare). O succesiune logică de posturi de lucru, conform intereselor de prelucrare urmărite, formează un circuit informaţional. Ansamblul informațiilor care se transmit între două posturi succesive de lucru formează un flux informaţional. Se remarcă suprapunerea sistemului informaţional atât peste sfera sistemului de conducere, cât şi peste cea a sistemului condus. În acest context, *sistemul informaţional* cuprinde: *circuitele informaţionale*, *fluxurile informaţionale*, *metodele şi tehnicile de prelucrare a informațiilor*.

Fiecare element al sistemului informaţional trebuie ştiinţific fundamentat, în raport de cerinţele (necesităţile) reale ale procesului conducerii şi execuţiei, astfel încât să faciliteze furnizarea la timp a informaţiei la locul de decizie. Când această cerinţă nu se poate asigura în condiţii optime, datorită verigilor intermediare prea numeroase, se impune reanalizarea întregii structuri organizatorice, în vederea mutării locului de decizie mai aproape de sursa de informaţii. Astfel circuitele informaţionale trebuie analizate şi scurtate pe cât posibil, de asemenea, fluxul informaţional trebuie să conţină elementele semnificative, evitând circulaţia unor date cu caracter de balast sau care sunt multiplicate în cadrul altor circuite (informații redondante). Având în vedere necesitatea optimizării managementului informațiilor dintr-o organizație, au apărut discipline specifice referitoare la reingineria proceselor într-o organizație.

În cadrul organizației, fluxurile şi circuitele informaţionale se integrează organic cu celelalte fluxuri şi circuite ale resurselor, astfel încât informațiile constituie un adevărat "liant" între diferitele componente ale organizației. În acest mod, sistemul informaţional, care întreţine aceste fluxuri şi circuite informaţionale, permite celorlalte sisteme să funcţioneze ca un *sistem integrat*. Modalităţile prin care sistemul informaţional îşi îndeplineşte obiectivele sale sunt în principal următoarele:

- ✓ asigură informațiile necesare fiecăruia dintre componentele organizației (sistemele de resurse), precum şi organziația percepută ca sistem în ansamblu;
- ✓ stabileşte modalităţile de colectare a datelor necesare fiecărei componente a sistemului pe care îl deservește;
- ✓ menţine colecţiile de date necesare pentru fundamentarea procesului decizional;
- ✓ generează informaţiile de ieşire care reflectă funcţionarea componentelor organizației, inclusiv ale sistemului informaţional însuşi.

Sistemul informațional este definit conform Standardului ISO 27000:2018 ca fiind un set de aplicații, servicii active în tehnologia informației sau alte componente de gestionare a informațiilor.

Având în vedere dinamica accentuată a tehnologiilor informaționale și de comunicații, transformarea digitală reprezintă modul de răspuns la provocările actuale pentru a asigura eficiența și performanța oricărei organizații. Astfel, procesul de management informațional este bazat pe sistem informatice performante care permit prelucrarea rapidă a unui volum mare de date (inclusiv big data), interpretarea acestora (analize de date – business intelligence). În plus, comunicația deschisă și globalizată care a condus la crearea spațiului cibernetic a creat noi provocări, ceea ce înseamnă dezvoltarea unei game largi de servicii și tranzacții online, în mod mult mai eficient, dar și facilități de accesare facilă și transfer rapid a informațiilor. În acest context, pe lângă avantajele incontestabile ale proceselor digitale, apar și riscuri semnificative cu privire la securitatea informațiilor.

În plus, sistemele informatice, indiferent de tehnologia pe care se bazează, gestionează un volum semnificativ de date cu caracter personal, deci în consecință se impune o atenție sporită acordată modului în care se realizează acest lucru. Astfel, aspectele legate de gestionarea datelor cu caracter personal trebuie avute în vedere încă din faza de proiectare a sistemului informatic, iar în cazul în care sistemul este în funcțiune, trebuie făcută analiza acestuia și luate măsuri de reproiectare pentru a se implementa cerințele specifice GDPR. Ca exemplu se pot menționa următoarele aspecte, legate de cerințele art. 25, respectiv asigurarea protecției datelor chiar din momentul conceperii acestora și în mod implicit. Acest fapt implică analiza datelor personale necesare pentru îndeplinirea misiunii/mandatului organizației, astfel încât să fie colectate, prelucrate și stocate informațiile minimum necesare. În cazul în care sunt colectate mai multe date personale decât cele strict necesare, trebuie reproiectate structurile de date, astfel încât să fie reduse la datele strict necesare. În plus, trebuie clar analizate prelucrările efectuate, inclusiv generarea de liste/rapoarte care pot cuprinde date cu caracter personal, pentru a asigura pseudonimizarea acestora. Mai mult, perioada de stocare reprezintă o altă cerință care trebuie respectată cu strictețe, în funcție de temeiul legal și misiunea/mandatul organizației. Cu privire la accesarea datelor cu caracter personal, aceasta trebuie restricționată, fiind permisă doar persoanelor care au responsabilități în acest sens (principiul “need to know”). Rezultă deci, că încă din faza de analiză și proiectare a unui sistem informatic sau la reproiectarea acestuia trebuie definite structurile de date și funcțiile de accesare, prelucrare și stocare a datelor cu caracter personal în concordanță cu cerințele stipulate la art. 25.

1.2 Securitatea informațiilor

Securitatea informațională reprezintă o măsură a încrederii utilizatorului asupra păstrării integrităţii atât a datelor, cât şi a sistemului de calcul.

Securitatea sistemelor informatice reprezintă protecția valorilor informaţionale faţă de o a accesare, modificare sau distrugere neautorizată, fie accidentală sau intenţionată, precum şi faţă de imposibilitatea accesului autorizat. Aceste cerințe se aplică și în cazul datelor cu caracter personal, așa cum este precizat la art. 32 al Regulamentului (UE) 2016/679.

Având în vedere procesul actual de transformare digitală, securitatea informațională și respectiv managementul securității informaționale depășește perspectiva tehnică legată de soluțiile de prevenire a unor incidente de securitate informațională, reprezentând o responsabilitate managerială. Ca urmare, pentru a gestiona aspectele multiple legate de securitatea informațională este necesar un Sistem de Management al Securității Informaționale (SMSI), care include luarea unor decizii potrivit evaluării contextului, precum și elaborarea unor politici, proceduri, sistem de analiză a riscurilor, a incidentelor de securitate și asigurarea coninuității activiății.

Poziția organizației referitoare la securitatea informației trebuie exprimată în *Politica de Securitate a Informaţiei și Politica de Securitate IT*, care stabilesc cu claritate politicile, principiile şi standardele specifice privind securitatea, precum şi cerinţele de conformitate cu acestea, controalele detaliate privind securitatea, responsabilităţile și sarcinile personalului în ceea ce privește securitatea informațiilor și securitatea IT, modalităţile de raportare în caz de incidente.

Informaţia este un activ care, ca şi alte active importante pentru o organizație, prezintă o valoare pentru organizație și, în consecinţă, trebuie protejată adecvat.

Informația este caracterizată de următoarele atribute fundamentale:

- **Confidențialitate**

  Confidențialitatea – protecția informațiilor în sistem astfel încât persoane neautorizate să nu le poată accesa, respectiv proprietatea ca informațiile să nu fie puse la dispoziție sau dezvăluite unor persoane, entități sau procese neautorizate. Este vorba despre controlarea dreptului de a accesa informațiile. Aproape fiecare organizație are informații care, dacă sunt divulgate sau furate, ar putea avea un impact semnificativ asupra avantajului competițional, valorii de piață sau a veniturilor. Adițional, o organizație poate fi facută responsabilă pentru divulgarea de informații private.

  Din perspectivă pragmatică, în cazul sistemelor informatice, pentru asigurarea confidențialității se utilizează:

  - controlul accesului pe baza unor tehnici de autentificare prin diferite metode (parole, coduri pin, token-uri, carduri inteligente etc.) și politici de restricționare a drepturilor de acces la acele informații absolut necesare, conform atribuțiilor și responsabilităților angajaților
  - tehnici de criptare pentru prevenirea accesului la informațiile reale, în cazul unui acces neautorizat sau fraudulos la acele informații

- **Integritate**

Integritatea – proprietatea datelor de a fi corecte (prelucrate cu acuratețe) și complete[80]. Astfel, se pune problema protecției informațiilor împotriva modificărilor intenționate sau accidentale neautorizate. Este vorba despre nevoia de a asigura că informația și programele sunt modificate numai în maniera specificată și autorizată și că datele prezente sunt originale, nealterate sau șterse în tranzit. Ca și în cazul confidențialității, identificarea și autentificarea utilizatorilor sunt elemente cheie ale unei politici de integritatea a informațiilor.

Din perspectivă pragmatică, în cazul sistemelor informatice, pentru asigurarea integrității se utilizează:

- tehnici de verificare a integrității datelor din bazele de date care deservesc un sistem informatic
- tehnici de verificare a transferului de date, pentru a se garanta că mesajul trimis nu a fost modificat sau alterat pe parcursul comunicării. Acest lucru este realizat, de obicei, prin atașarea la mesaj a unui șir de control (digest, hash) de lungime fixă. Acest șir de control poate fi recreat de către destinatar și permite identificarea unei modificări intenționate sau nu a conținutului mesajului trimis.

- **Disponibilitate**

Disponibilitatea - se referă la asigurarea că sistemele de calcul sunt accesibile utilizatorilor autorizați când și unde aceștia au nevoie și în forma necesară (informația stocată electronic este unde trebuie să fie, când trebuie să fie acolo și în forma necesară).

Din perspectivă pragmatică, în cazul sistemelor informatice, pentru asigurarea disponibiliății se utilizează:

- tehnici de redundanță (rutere, hard discuri)
- tehnici de backup (copiere de suporturi externe și pe cel puțin 2 suporturi diferite, stocate în locuri diferite)
- soluții anti-malware

- **Autenticitate**

Autenticitatea informației - este acea proprietate a sistemului sau a rețelei de a permite asocierea informației cu sursa legală de producere a ei.

Din perspectivă pragmatică, în cazul sistemelor informatice, pentru asigurarea autenticității se utilizează:

- tehnici de autentificare
- tehnici de criptare

[80] Standard ISO 27000:2018

- **Nerepudiere**

Nerepudierea informației - este acea proprietate a sistemului sau a rețelei de a asocia informației dovada că informația a fost transmisă de o entitate identificată și a fost recepționată de o altă entitate identificată fără posibilitate de contestare.

Din perspectivă pragmatică, în cazul sistemelor informatice, pentru asigurarea autenticității se utilizează:

- tehnici de autentificare
- tehnici de criptare

Terminologia în domeniul securității informaționale este definită în cadrul sandardului ISO 27000 : 2018. Principalele concepte utilizate în domeniul securității informaționale sunt prezentate în cele ce urmează:

- **Amenințare** – cauză potențială nedorită a unui incident nedorit, care poate duce la vătămarea unui sistem sau a unei organizații.
- **Atac** – acțiune care încearcă să distrugă, să expună, să modifice, să dezactiveze, să fure sau să obțină acces neautorizat sau să utilizeze neautorizat un activ.
- **Eveniment de securitate a informațiilor** – identificarea apariției unui sistem, serviciu sau stare a rețelei care indică o posibilă încălcare a politicii de securitate a informațiilor sau eșecul controalelor sau o situație necunoscută anterior care poate fi relevantă pentru securitate.
- **Incident de securitatea informațiilor -** reprezintă un eveniment sau o serie de evenimente nedorite sau neașteptate de securitate a informațiilor care au o probabilitate semnificativă de a compromite operațiunile comerciale și de a amenința securitatea informațiilor.
- **Vulnerabilitate -** reprezintă slăbiciunea unui activ sau control[81].

1.3 Sistemul de management al securității informațiilor

Asigurarea securității înformațiilor gestionate înseamnă evaluarea situației și luarea unor decizii corecte, pe baza unui sistem de management al securității informațiilor – SMSI - bazat pe politici, proceduri, analiza riscurilor, a incidentelor de securitate și asigurarea continuității activității.

Managementul Securități include:

- Clasificarea informațiilor
- Organizarea structurii de securitate în organizație (ierarhia)
- Ghiduri- Standarde (aplicabile in organizație)
- Politicile de securitate
- Procedurile de securitate
- Managementul riscului
- Educația personalului privind securitatea informațiilor

[81]Măsură care modifică/ameliorează riscurile. Conroalele include orice proces, politică, dispozitiv, practică sau orice actiune care modifică riscul. Este posibil ca aceste controale să nu exercite întotdeauna efectul modificator intenționat sau presupus.

Managementul securității informației se definește ca fiind ansamblul proceselor de stabilire și menținerea unui cadru de lucru și a unei structuri de administrare care oferă garanția că strategiile de securitatea informației sunt aliniate și susținute prin obiectivele organizației, sunt în concordanță cu legile și reglementările aplicabile pentru administrarea cât mai adecvată a riscurilor.

Un **Sistem de Management al Securității Informației (SMSI)** include (conform ISO 27001 pentru securitatea informației[82]) **toate politicile, procedurile, planurile, procesele, practicile, rolurile, responsabilitățile, resursele și structurile** care sunt folosite pentru a **proteja și păstra intactă informația**. SMSI integrează astfel:

- toate elementele pe care organizațiile le folosesc pentru a-și gestiona și a-și controla riscurile legate de securitatea informației;
- toate măsurile pentru protejarea informațiilor pe tot ciclul lor de viață, indiferent de forma informațiilor și de mediul specific de comunicare utilizat.

Un **SMSI** este o parte integrantă a sistemului de management al organizației și acoperă întreaga arie informațională (asigură securitatea tuturor informațiilor, indiferent dacă sunt în format digital sau nu). Este important de subliniat că **adoptarea unui SMSI** trebuie să fie o **decizie strategică** pentru organizație deoarece:

- SMSI nu este un instrument pentru specialiștii IT și nicipentru specialiștii în securitate informatică, ci al **managementului de vârf.**
- SMSI susține managementul de vârf în conștientizarea riscurilor de securitate a informației prin:
  - informarea asupra **riscurilor rezultate din utilizarea informației** în procesele de producție pentru a putea să determine relevanța și nivelul critic al acesteia în conformitate cu cerințele afacerii.
  - posibilitatea de a decide în cunoștință de cauză cum trebuie să **controleze riscurile** prin **planificarea, implementarea și monitorizarea măsurilor** luate pentru a **evita, reduce și transfera riscurile**, și pentru a fi capabil de a **administra incidentele posibile**.

Standardul I.S.O. / I.E.C. 27001:2018 "Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației" este cel mai cunoscut document normativ în vederea implementării și certificării unui S.M.S.I. într-o organizație. Acest standard stabilește cerințele pentru un Sistem de Management al Securității Informației și ajută la identificarea, managementul și minimizarea amenințărilor care afectează de obicei informația.

Standardul include următoarele:

- ✓ formularea cerințelor de securitate și a obiectivelor;
- ✓ asigurarea ca riscurile de securitate sunt controlate și "stăpânite" din punct de vedere al costului;
- ✓ asigurarea unei conformități cu legislația și diverse reglementări;
- ✓ identificarea și clarificarea proceselor existente de management al securității informației;

[82]**SR ISO/CEI 27001:2018**, Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației

- ✓ utilizarea de către management pentru a determina statusul activităților de management al securității informației;
- ✓ utilizarea de către auditori interni și externi pentru a determina gradul de conformitate cu politicile, directivele și standardele adoptate de către organizație;
- ✓ furnizarea de informații relevante despre politicile de securitatea informației, standarde si proceduri, către parteneri.

Standardul are la bază următoarele principii care definesc securitatea informației:

- confidențialitatea;
- integritatea;
- disponibilitatea informației.

Acest standard asigură o abordare pe termen lung a securității, bazându-se pe implementarea de politici, proceduri și metode de securitate destinate protejării informațiilor și resurselor organizațiilor.

Prin reducerea la maximum a riscurilor, se garantează că sistemul de management al securității informațiilor este funcțional și indeplinește cerințele operaționale ale organizației, asteptările partenerilor și beneficiarilor și se conformează legislației în vigoare. Totodată, ISO/ IEC 27001 este aliniat cu ISO 9001, dar şi cu ISO 14001, asigurând astfel premisele unui management integrat.

În plus, **Sistemul de management al securității informaționale (SMSI)** se bazează pe o serie de standarde internaționale din familia 27000 (parțial cu titu de exemplu):

- **ISO / IEC 27000:2018**, Sisteme de management al securitatii informațiilor ISO - Prezentare generală și vocabular
- ***ISO / IEC 27001:2018**, Sistem de management al securității informației - Cerințe*
- ***ISO / IEC 27002:2018**, Codul de practică pentru controalele de securitate a informațiilor*
- ***ISO / IEC 27003:2013**, managementul de securitate informațională de orientare si implementare a sistemului*
- ***ISO / IEC 27004:2016**, de management al securității informației – Măsurarea/ Evaluarea*
- **ISO / IEC 27005*:2016***, Managementul riscului de securitate informațională
- **ISO / IEC 27007*:2016***, Linii directoare pentru sistemele de management al securitatii informatiei și de audit
- **ISO / IEC 27011**, liniile directoare de management al securității informațiilor pentru organizațiile de telecomunicații pe baza ISO / IEC 27002
- ***ISO / IEC 27701:2019***, Tehnici de securitate – Extensie la *ISO/IEC 27001 și ISO/IEC 27002 pentru managementul informațiilor private* - Cerințe și linii directoare

Cu privire la managementul securității informaționale, din perspectivă pragmatică, sunt abordate aspectele referitoare la:

- **Securitatea fizică**
- **Securitatea logică**
- **Securitatea personalului**
- **Asigurarea continuității afacerii/serviciului**

În plus, sistemul de management al securității informaționale se extinde și se particularizează în domeniul informațiilor cu caracter personal, identificându-se sistemul de management al informațiilor cu caracter privat. ISO/IEC 27701 realizează integrarea aspectelor referitoare la securitatea informațiilor cu cerințele specifice implicate de managemenul datelor cu caracter personal, oferind un cadru de gestionare a datelor cu caracter personal care poate fi utilizat atât de operatorii de date, cât și de procesatorii de date, în conformitate cu GDPR.

1.4 Organizarea securității informației

Cultura de securitate în interiorul unei organizații este un proces de durată ce poate fi dezvoltat prin impunerea unor măsuri și/sau mecanisme de securitate care să minimizeze riscurile ce pot să apară în procesele din cadrul organizației. Fiecare activitate este guvernată de amenințări, vulnerabilități și riscuri. În momentul în care un risc depășește un anumit nivel acceptat avem de-a face cu un incident de securitate care trebuie rezolvat (tratarea riscului pâna când se încadrează sub nivelul acceptat).

Organizarea securității rezolvă cel puțin două aspecte de bază:

- Clasifică informațiile / resursele critice;
- Stabilește responsabilități de securitate și implicarea top managementului pentru gestionarea incidentelor de securitate și planificarea continuității activităților organizației în caz de dezastre sau evenimente majore.

Funcție de mărimea, procesele din organizație și specificul activității desfășurate, organizarea internă a securității este o activitate continuă și complexă.

2. Prelucrarea datelor cu caracter personal în sistemul MySMIS 2014

MySMIS 2014 reprezintă un sistem informatic utilizat ca un instrument în gestiunea proiectelor finanțate din ***Fonduri Europene Structurale și de Investiții (FESI)*** de către Ministerul Investițiilor și Proiectelor Europene (MIPE), Autoritățile de Management al Programelor Operationale (AM), Organizmele Intermediare (OI), Beneficiarii proiectelor cu finanțarte Europeană.

Având în vedere natura și scopul sistemului MySMIS 2014 și anume colector și gestionar de informații inclusiv de date cu caracter personal, se impune respectarea de către acesta a unor standarde ridicate de protecție a datelor cu caracter personal și a celorlalte informații gestionate.

În vederea asigurării sistemului MySMIS 2014 la conformarea cerută de GDPR, este necesar crearea și implementarea unui plan de asigurare a conformității sistemului care să treacă cel puțin prin următoarele etape:

- Cartografierea (inventarierea) prelucrărilor care se efectuează la nivelul sistemului MySMIS 2014;
- Evaluarea impactului asupra protecției datelor personale- DPIA;
- Aplicarea recomandărilor DPIA, prin revizuirea prelucrărilor de date cu caracter personal, astfel încât să se diminueze riscurile la adresa drepturile și libertățile persoanelor fizice;

- Revizuirea prelucrărilor de date cu caracter personal realizateîn cadrul sistemului MySMIS 2014 în vederea aplicării principiilor GDPR;
- Pentru prelucrările care au ca și temei interesul legitim se recomandă realizarea unei Analize a Interesului Legitim (LIA);
- Pentru sistemul MySMIS 2014 trebuie adoptate mecanisme și proceduri proprii, privind gestionarea drepturilor persoanelor vizate;
- Implementarea politicilor și procedurilor avizate;
- Implementarea măsurilor tehnice și organizatorice privind securitatea datelor cu caracter personal.

Cartografierea prelucrărilor care se efectuează de către sistemul MySMIS 2014, presupune identificarea a cel puțin:

- Scopul prelucrărilor;
- Categoriile de date cu caracter personal prelucrate;
- Categoriile de persoane vizate;
- Temeiurilor de prelucrare;
- Destinatari, inclusiv din afără Spațiului Economic European pentru transferurile de date cu caracter personal;
- Stabilirea termenelor limită de păstrare a datelor personale;
- Aplicarea consecventă a măsurilor tehnice și organizatorice stabilite și implementate.

Evaluarea impactului asupra protecției datelor personale DPIA - este necesară în cazul în care un tip de prelucrare – în mod special cele în care se utilizează noi tehnologii – poate genera un risc ridicat pentru drepturile și libertățile persoanelor fizice[83].

Aplicarea recomandărilor DPIA, prin revizuirea prelucrărilor de date cu caracter personal astfel încât să se diminueze riscurile la adresa drepturile și libertățile persoanelor fizice.

Revizuirea prelucrărilor de date cu caracter personal realizate în cadrul sistemului MySMIS 2014 în vederea aplicării principiilor GDPR:

- Principiul de legalitate și scop;
- Principiul limitării legate de scop;
- Principiul reducerii la minim a datelor cu caracter personal, doar la ceea ce este strict necesar realizării scopului definit.

Pentru sistemul MySMIS 2014 trebuie adoptate și implementate mecanisme și proceduri proprii, privind gestionarea drepturilor persoanelor vizate, care se referă la cel puțin:

- Identificarea categoriilor de persoane vizate;
- Elaborarea formularelor de notificare și informare a categoriilor de persoane vizate aplicându-se principiul transparenței;
- Elaborarea formularelor de colectare a consimțământului persoanelor vizate, acolo unde prelucrarea se bazează pe consimțământ;
- Stabilirea modalității de informare și obținere a consimțământului persoanelor vizate;
- Stabilirea modalității de elaborare a registrului privind consimțământul persoanelor vizate și actualizarea lui;

[83] Regulamenul (UE) 2016/679 - art. 35 (1)

- Stabilirea modalității de informare atunci când au loc modificări la nivelul notificărilor de informare sau elaborarea unei proceduri de informare periodică;
- Elaborarea procedurii de exercitare a drepturilor persoanelor vizate;
- Elaborarea registrului privind evidența cererilor persoanelor vizate.

Implementarea politicilor și procedurilor, presupune realizarea și implementarea acestora și se referă cel puțin la:

- Politica de securitate a informațiilor și datelor cu caracter personal
- Politica de protecție a datelor cu caracter personal
- Procedura de exercitare a drepturilor persoanelor vizate
- Politica privind cookies
- Politica și/sau Procedura de instruire a utilizatorilor în domeniul protecției datelor cu caracter personal la nivelul sistemului MySMIS 2014
- Procedura de evaluare a furnizorilor
- Procedurile de ștergere, anonimizare și pseudoanonimizare
- Politica ***Privacy by Design*** și ***By Default***
- Procedura privind gestionarea incidentelor de securitate la adresa datelor cu caracter personal

Implementarea măsurilor tehnice și organizatorice privind securitatea datelor cu caracter personal, la nivelul sistemul informatic MySMIS 2014 presupune cel puțin:

❑ ***Managementul accesului*** care presupune:

- Implementarea de politici de securizare a accesului la sistem prin definirea unei matrici de acces, prin separarea sarcinilor și responsabilităților; Aceasta trebuie să țină cont și de drepturile de descărcare a documentelor stocate în sistem;
- Implementarea unor politici/proceduri de acces la bazele de date, serverele de aplicații astfel încât doar personalul autorizat să aibă acces la acele resurse;
- Implementarea de proceduri de retragere/restrângere a accesului utilizatorilor de îndată ce aceștia nu mai sunt autorizați să utilizeze parțial sau total respectivele resurse;
- Efectuarea unei analize anuale sau de câte ori se impune privind drepturile de acces.

Matricea de control privind nivelul de acces

Subiect	Obiect		
	1	2	3
A	Execută	Citește	Citește/Scrie
B	Aprobă	Execută	Citește
C	Citește/Scrie	Aprobă	Execută

D	Citește	Citește/Scrie	Aprobă
E	Execută	Citește	Citește/Scrie

- ***Autentificarea utilizatorilor:***

  - Definirea pentru fiecare utilizator a unui identificator unic
  - Aplicarea de politici de securizare a parolei

- ***Monitorizarea accesului*** şi ***managementul incidentelor de securitate:***

  - Configurarea jurnalelor pentru înregistrarea activității utilizatorilor, anomaliilor și evenimentelor legate de securitate;
  - Implementarea unei proceduri de jurnalizare a accesului furnizorilor externi de servicii IT pe serverele unde este găzduit sistemul, astfel încât să existe o trasabilitate a acțiunilor întreprinse;
  - Monitorizarea utilizării sistemului și efectuarea de analize în vederea identificării anomaliilor sau accesărilor neautorizate;
  - Implementarea unui serviciu de evaluare și scanare periodică a vulnerabilităților sistemelor IT - Vulnerability Assessment and Management
  - Realizarea de teste de penetrare a rețelei atât din Internet, cât și din interiorul rețelei pentru a testa reziliența sistemelor IT la atacurilor malițioase și descoperirea de vulnerabilități;
  - Realizarea și implementarea unei proceduri de tratare a incidentelor de securitate.

- ***Protejarea stațiilor de lucru*** ale utilizatorilor sistemului MySMIS 2014, în special pentru cei care au drepturi de descărcare documente din sistem

  - Implementarea de politici de securitate pentru accesul la stațiile de lucru, prin acces pe baza de user și parola. Crearea de conturi nominale pentru utilizatori și dezactivarea celor cu nume generic
  - Aplicarea de politici de securizare a parolei, schimbare acesteia la un interval de timp predefinit;
  - Stațiile de lucru configurate să se blocheze automat în momentele de inactivitate și la reluarea activității să solicite userul și parola utilizatorului, pentru a preveni accesul neautorizat la stațiile de lucru;
  - Stabilirea politicilor/procedurilor de acces cu memory stik-uri sau alte echipamente portabile de stocare a datelor la nivelul stațiilor de lucru;
  - Acceptarea transferului de date doar către echipamentele portabile acceptate în instituție;
  - Criptarea acestor echipamente portabile de transfer a datelor;
  - Acceptarea transferului de date de la sau doar către echipamentele cu IP-uri autorizate și recunoscute;
  - Eliminarea programelor antivirus gratuite de pe computerele utilizatorilor și înlocuirea/implementarea unei soluții antivirus performante cu suport din partea producătorului și cu consola de management centralizat, ce permite monitorizarea în timp real a situației actualizărilor semnăturilor;
  - Eliminarea programelor de acces de la distanță de pe stațiile de lucru fără VPN
  - Asigurarea accesului de la distanță numai pe servere și cu acces VPN.

- ***Protejarea reţelei interne***

  - Limitarea accesului la serviciile neesențiale (VoIP, peer to peer)
  - Gestionarea rețelelor Wi-Fi prin utilizarea celor mai noi tehnologii de criptare (WPA2 sau WPA2-PSK cu parole complexe);
  - Implementarea unui VPN pentru acces la distanță, precum și, dacă este posibil, o metodă de autentificare complexă a utilizatorului (parolă unică generată de fiecare dată);
  - Asigurarea că nicio interfață de administrare nu este direct accesibilă de pe Internet, iar întreținerea la distanță este realizată obligatoriu printr-o rețea VPN

- ***Asigurarea continuităţii activităţii***

  - Proceduri de backup, implementare sisteme securitate, firewall
  - Efectuarea de copii de siguranță (backup), periodic, protejarea acestora asigurând același nivel de securitate ca și cel pentru datele stocate pe serverele operaționale;
  - Testare periodică a vulnerabilităților și punerea în aplicare a Planului de Continuitate în caz de dezastre sau evenimente majore
  - Achiziționarea de generatoare/UPS-uri pentru serverele locale
  - Contractarea şi impunerea asigurării continuităţii furnizării energiei electrice la serverele de stocare
  - Utilizarea unei surse de alimentare continuă pentru a proteja echipamentele TIC utilizate
  - Implementarea unui provider secundar de Internet, care să asigure funcționalitatea continuă a serviciului de acces la Internet

- ***Stocarea și arhivarea electronică a documentelor în mod securizat:***

  - Elaborarea și implementarea unei proceduri de gestionare a arhivei electronice, incluzând metode specifice de acces la datele arhivate electronic;
  - Măsuri de asigurare back-up la toate documente care conțin informații importante și date cu caracter personal;
  - Aplicarea de măsuri care să garanteze distrugerea arhivei electronice în întregimea sa, inclusiv backup-ul arhivelor ajunse la scadența retenției.

Securizarea serverului

Securizarea serverului presupune controlarea cererilor care i-au fost adresate şi securizarea sistemului informatic cu care colaborează pentru a înapoia serviciul solicitat de clienţi. Plecând de la stricta configurare a sistemului, protejarea acestuia de exterior se face de obicei prîntr-un *firewall*. Configurarea unui *firewall* se face după criteriile de securitate determinate pentru filtrarea traficului parcurs şi astfel se aplică o politică de control al accesului la sistem. Protejarea datelor constă, deci, în limitarea accesului la acestea, precum şi punerea lor la dispoziţia clienţilor autorizaţi.

- Serverele:

  - Sincronizarea ceasurilor tuturor echipamentelor din infrastructura TIC cu același server de tip NTP (Network Time Protocol) - Echipamente de rețea, servere, stații de lucru, echipamente mobile

- Asigurarea unei temperaturi optime de lucru pentru echipamentele din camera serverelor
- Asigurarea protecției fizice adecvate pentru echipamentele din camera unde sunt găzduite serverele
- Asigurarea protecției fizice adecvate pentru echipamentele de tip DVR/NVR. Securizarea lor în rack-uri specializate
- Verificarea echipamentelor de protecție împotriva vârfurilor de tensiune – UPS-urile, din camera serverelor
- Realizarea de teste de performanță și înlocuirea lor acolo unde este cazul. Conectarea pe cât posibil a tuturor echipamentelor la UPS-uri
- Realizarea unui jurnal cu evidențe de acces în această cameră, pentru a avea trasabilitatea accesului fizic la serverele pe care sunt gazduite sistemele și platformele informatic

Aplicația MySMIS, dezvoltată de Ministerul Fondurilor Europene și STS, poate fi utilizată de toate organizațiile care doresc să depună proiecte cu finanțare din fonduri europene nerambursabile.

Ca o măsură suplimentară de asigurare a securității informațiilor și datelor cu caracter personal introduse de Solicitanții (Beneficiarii) de fonduri Europene nerambursabile în vederea implementării proiectelor aprobate spre finanțare, din martie 2016, a fost introdus în mod obligatoriu certificatul digital calificat emis de certSIGN, care este utilizat pentru semnarea electronică a tuturor documentelor necesare a fi încărcate în aplicația MySMIS.

Pentru a fi acceptate de sistem, documentele vor fi semnate electronic – lucru care le asigură autenticitatea, integritatea și non-repudierea, utilizând certificatul digital calificat al beneficiarului fondurilor europene sau al unei persoane împuternicite de acesta.

Capitolul VII. CONSECINȚELE NERESPECTĂRII PREVEDERILOR REGULAMENTULUI GENERAL PRIVIND PROTECȚIA DATELOR (GDPR)

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 prevede la capitolul VIII - Căile de atac, răspunderea și sancțiunile care se aplica pentru incalcarea prevederilor Regulamentului

În conformitate cu prevederile Articolului 77 – este garantat dreptul fiecărei persoane vizate de a depune o plângere la o autoritate de supraveghere.

Astfel, fără a aduce atingere oricăror alte căi de atac administrative sau judiciare, orice persoană vizată are dreptul de a depune o plângere la o autoritate de supraveghere, în special în statul membru în care își are reședința obișnuită, în care se află locul său de muncă sau în care a avut loc presupusa încălcare, în cazul în care consideră că prelucrarea datelor cu caracter personal care o vizează încalcă prezentul regulament.

Autoritatea de supraveghere la care s-a depus plângerea are obligația de a informa reclamantul cu privire la evoluția și rezultatul plângerii, inclusiv posibilitatea de a exercita o cale de atac judiciară în temeiul articolului 78 din Regulament.

Cum se poate formula o plângere la autoritatea de supraveghere ?

Pe site-ul autorității de supraveghere www.dataprotection.ro este disponibil un formular electronic de plângere la secțiunea Plângeri.

Procedura de primire și soluționare a plângerilor este reglementată de prevederile Deciziei nr. 133/2018 a Președintelui Autorității de supraveghere[84]

Când este admisibilă o plângere ?

Potrivit Deciziei nr. 133/2018 și în concordanță cu Legea nr. 102/2005 privind înființarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările și completările ulterioare, pentru primirea şi înregistrarea valabilă a plângerilor este obligatorie furnizarea următoarelor date ale petiţionarului: nume, prenume, adresă poştală de domiciliu sau de reşedinţă. În cazul în care plângerea este depusă electronic este obligatorie furnizarea adresei de poştă electronică a petiţionarului.

În cazul plângerilor înaintate prin reprezentant, în afara datelor petiţionarului menționate la alin. (1), este obligatorie şi furnizarea următoarelor date ale reprezentantului: nume şi prenume/denumire, adresă poştală de corespondenţă/sediu, adresă de poştă electronică, număr de telefon, număr de înregistrare în registrul asociaţiilor şi fundaţiilor, dacă este cazul.

Pentru primirea şi înregistrarea valabilă a plângerilor este obligatorie furnizarea datelor de identificare ale operatorului reclamat sau a persoanei împuternicite reclamate, precum nume şi prenume/denumire, adresă/sediu, sau cel puţin a informațiilor disponibile deţinute de petiţionar, în vederea identificării acestora.

Plângerile trimise se semnează olograf sau electronic, iar în cazul petițiilor trimise electronic care nu pot fi semnate, ANSPDCP poate solicita confirmarea corectitudinii datelor transmise electronic.

Autoritatea națională de supraveghere informează persoana vizată cu privire la admisibilitatea plângerii, în termen de cel mult 45 de zile de la înregistrare. În cazul în care se constată că informațiile din plângere sau documentele transmise sunt incomplete sau insuficiente, Autoritatea națională de supraveghere solicită persoanei vizate să completeze plângerea pentru a putea fi considerată admisibilă în vederea efectuării unei investigații. Un nou termen de cel mult 45 de zile curge de la data completării plângerii.

[84] Site ANSPDCP

Autoritatea națională de supraveghere informează persoana vizată în legătură cu evoluția sau cu rezultatul investigației întreprinse în termen de 3 luni de la data la care s-a comunicat acesteia că plângerea este admisibilă.[85]

Un alt drept prevazut de Rregulament la articolul 78, este Dreptul la o cale de atac judiciară eficientă împotriva unei autorități de supraveghere.

Astfel fiecare persoană fizică sau juridică are dreptul de a exercita o cale de atac judiciară eficientă împotriva unei decizii obligatorii din punct de vedere juridic a unei autorități de supraveghere care o vizează, fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare.

Fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care autoritatea de supraveghere care este competentă în temeiul articolelor 55 și 56 nu tratează o plângere sau nu informează persoana vizată în termen de trei luni cu privire la progresele sau la soluționarea plângerii depuse în temeiul articolului 77.

Acțiunile introduse împotriva unei autorități de supraveghere sunt aduse în fața instanțelor din statul membru în care este stabilită autoritatea de supraveghere, iat in cazul în care acțiunile sunt introduse împotriva unei decizii a unei autorități de supraveghere care a fost precedată de un aviz sau o decizie a comitetului în cadrul mecanismului pentru asigurarea coerenței, autoritatea de supraveghere transmite curții avizul respectiv sau decizia respectivă.[86]

Articolul 79 reglementează dreptul la o cale de atac judiciară eficientă împotriva unui operator sau unei persoane împuternicite de operator.[87]

Fără a aduce atingere vreunei căi de atac administrative sau nejudiciare disponibile, inclusiv dreptului de a depune o plângere la o autoritate de supraveghere în temeiul articolului 77, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care consideră că drepturile de care beneficiază în temeiul prezentului regulament au fost încălcate ca urmare a prelucrării datelor sale cu caracter personal fără a se respecta prezentul regulament.

De asemenea, acțiunile introduse împotriva unui operator sau unei persoane împuternicite de operator sunt prezentate în față instanțelor din statul membru unde operatorul sau persoana împuternicită de operator își are un sediu. Alternativ, o astfel de acțiune poate fi prezentată în față instanțelor din statul membru în care persoana vizată își are reședința obișnuită, cu excepția cazului în care operatorul sau persoana împuternicită de operator este o autoritate publică a unui stat membru ce acționează în exercitarea competențelor sale publice.

Dreptul de reprezentare a persoanelor vizate este prevăzut de articolul 80 din Regulament.

În conformitate cu prevederile acestui articol persoana vizată are dreptul de a

[85] Site ANSPDCP

[86] Art. 78 Regulamentului (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

[87] Art. 79 Regulamentului (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

mandata un organism, o organizație sau o asociație fără scop lucrativ, care au fost constituite în mod corespunzător în conformitate cu dreptul intern, ale căror obiective statutare sunt de interes public, care sunt active în domeniul protecției drepturilor și libertăților persoanelor vizate în ceea ce privește protecția datelor lor cu caracter personal, să depună plângerea în numele său, să exercite în numele său drepturile menționate la articolele 77, 78 și 79, precum și să exercite dreptul de a primi despăgubiri menționat la articolul 82 în numele persoanei vizate, dacă acest lucru este prevăzut în dreptul intern.

Statele membre pot prevedea că orice organism, organizație sau asociație menționată la alineatul (1) din prezentul articol, independent de mandatul unei persoanei vizate, are dreptul de a depune în statul membru respectiv o plângere la autoritatea de supraveghere care este competentă în temeiul articolului 77 și de a exercita drepturile menționate la articolele 78 și 79, în cazul în care consideră că drepturile unei persoane vizate în temeiul prezentului regulament au fost încălcate ca urmare a prelucrării.

Articolul 81 - Suspendarea procedurilor[88]

(1) În cazul în care o instanță competentă a unui stat membru are informații că pe rolul unei instanțe dintr-un alt stat membru se află o acțiune având același obiect în ceea ce privește activitățile de prelucrare ale aceluiași operator sau ale aceleași persoane împuternicite de operator, instanța respectivă contactează instanța din celălalt stat membru pentru a confirma existența unor astfel de acțiuni.
(2) Atunci când pe rolul unei instanțe dintr-un alt stat membru se află o acțiune având același obiect în ceea ce privește activitățile de prelucrare ale aceluiași operator sau ale aceleași persoane împuternicite de operator, orice altă instanță competentă decât instanța sesizată inițial poate suspenda acțiunea aflată la ea pe rol.
(3) În cazul în care o astfel de acțiune se judecă în primă instanță, orice instanță sesizată ulterior poate, de asemenea, la cererea uneia dintre părți, să-și decline competența, cu condiția ca respectiva acțiune să fie de competența primei instanțe sesizate și ca dreptul aplicabil acesteia să permită conexarea acțiunilor.

Articolul 82 - Dreptul la despăgubiri și răspunderea[89]

(1) Orice persoană care a suferit un prejudiciu materiale sau moral ca urmare a unei încălcări a prezentului regulament are dreptul să obțină despăgubiri de la operator sau de la persoana împuternicită de operator pentru prejudiciul suferit.
(2) Orice operator implicat în operațiunile de prelucrare este răspunzător pentru prejudiciul cauzat de operațiunile sale de prelucrare care încalcă prezentul regulament. Persoana împuternicită de operator este răspunzătoare pentru prejudiciul cauzat de prelucrare numai în cazul în care nu a respectat obligațiile din prezentul regulament care revin în mod specific persoanelor împuternicite de operator sau a acționat în afară sau în contradicție cu instrucțiunile legale ale operatorului.
(3) Operatorul sau persoana împuternicită de operator este exonerat(ă) de răspundere în temeiul alineatului (2) dacă dovedește că nu este răspunzător (răspunzătoare) în niciun

[88] Art. 81 Regulamentului (UE) 2016/679 al Parlamentului European și 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
[89] Art. 82 Regulamentului (UE) 2016/679 al Parlamentului European și 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

fel pentru evenimentul care a cauzat prejudiciul.
(4) 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, în temeiul alineatelor (2) și (3), 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.
(5) În cazul în care un operator sau o persoană împuternicită de operator a plătit, în conformitate cu alineatul (4), 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, în conformitate cu condițiile stabilite la alineatul (2).

(6) Acțiunile în exercitarea dreptului de recuperare a despăgubirilor plătite se introduc la instanțele competente în temeiul dreptului statului membru menționat la articolul 79 alineatul (2).

Articolul 83 - Condiții generale pentru impunerea amenzilor administrative[90]

(1) Fiecare autoritate de supraveghere asigură faptul că impunerea unor amenzi administrative în conformitate cu prezentul articol pentru încălcările prezentului regulament menționate la alineatele (4), (5) și, (6) este, în fiecare caz, eficace, proporțională și disuasivă.

(2) În funcție de circumstanțele fiecărui caz în parte, amenzile administrative sunt impuse în completarea sau în locul măsurilor menționate la articolul 58 alineatul (2) literele (a)-(h) și (j). Atunci când se ia decizia dacă să se impună o amendă administrativă și decizia cu privire la valoarea amenzii administrative în fiecare caz în parte, se acordă atenția cuvenită următoarelor aspecte:

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

[90] Art. 83 Regulamentului (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

(h) modul în care încălcarea a fost adusă la cunoștința autorității de supraveghere, în special dacă și în ce măsură operatorul sau persoana împuternicită de operator a notificat încălcarea;
(i) în cazul în care măsurile menționate la articolul 58 alineatul (2) au fost dispuse anterior împotriva operatorului sau persoanei împuternicite de operator în cauză cu privire la același obiect, respectarea respectivelor măsuri;
(j) aderarea la coduri de conduită aprobate, în conformitate cu articolul 40, sau la mecanisme de certificare aprobate, în conformitate cu articolul 42; și
(k) orice alt factor agravant sau atenuant aplicabil circumstanțelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect de pe urma încălcării.

(3) În cazul în care un operator sau o persoană împuternicită de operator încalcă în mod intenționat sau din neglijență, pentru aceeași operațiune de prelucrare sau pentru operațiuni de prelucrare conexe, mai multe dispoziții din prezentul regulament, cuantumul total al amenzii administrative nu poate depăși suma prevăzută pentru cea mai gravă încălcare.

(4) Pentru încălcările dispozițiilor următoare, în conformitate cu alineatul (2), se aplică amenzi administrative de până la 10 000 000 EUR sau, în cazul unei întreprinderi, de până la 2 % din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare:

(a) obligațiile operatorului și ale persoanei împuternicite de operator în conformitate cu articolele 8, 11, 25-39, 42 și 43;
(b) obligațiile organismului de certificare în conformitate cu articolele 42 și 43;
(c) obligațiile organismului de monitorizare în conformitate cu articolul 41 alineatul (4).

5) Pentru încălcările dispozițiilor următoare, în conformitate cu alineatul (2), se aplică amenzi administrative de până la 20 000 000 EUR sau, în cazul unei întreprinderi, de până la 4 % din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare:

(a) principiile de bază pentru prelucrare, inclusiv condițiile privind consimțământul, în conformitate cu articolele 5, 6, 7 și 9;
(b) drepturile persoanelor vizate în conformitate cu articolele 12-22;
(c) transferurile de date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională, în conformitate cu articolele 44-49;
(d) orice obligații în temeiul legislației naționale adoptate în temeiul capitolului IX;
(e) nerespectarea unui ordin sau a unei limitări temporare sau definitive asupra prelucrării, sau a suspendării fluxurilor de date, emisă de către autoritatea de supraveghere în temeiul articolului 58 alineatul (2), sau neacordarea accesului, încălcând articolul 58 alineatul (1).

(6) Pentru încălcarea unui ordin emis de autoritatea de supraveghere în conformitate cu articolul 58 alineatul (2) se aplică, în conformitate cu alineatul (2) din prezentul articol, amenzi administrative de până la 20 000 000 EUR sau, în cazul unei întreprinderi, de până la 4 % din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar

anterior, luându-se în calcul cea mai mare valoare.[91]
(7) Fără a aduce atingere competențelor corective ale autorităților de supraveghere menționate la articolul 58 alineatul (2), fiecare stat membru poate prevedea norme prin care să se stabilească dacă și în ce măsură pot fi impuse amenzi administrative autorităților publice și organismelor publice stabilite în statul membru respectiv.
(8) Exercitarea de către autoritatea de supraveghere a competențelor sale în temeiul prezentului articol are loc cu condiția existenței unor garanții procedurale adecvate în conformitate cu dreptul Uniunii și cu dreptul intern, inclusiv căi de atac judiciare eficiente și dreptul la un proces echitabil.
(9) În cazul în care sistemul juridic al statului membru nu prevede amenzi administrative, prezentul articol poate fi aplicat astfel încât amenda să fie inițiată de autoritatea de supraveghere competentă și impusă de instanțele naționale competente, garantându-se, în același timp, faptul că aceste căi de atac sunt eficiente și au un efect echivalent cu cel al amenzilor administrative impuse de autoritățile de supraveghere. În orice caz, amenzile impuse trebuie să fie eficace, proporționale și disuasive. Respectivele state membre informează Comisia cu privire la dispozițiile de drept intern pe care le adoptă în temeiul prezentului alineat până la 25 mai 2018, precum și, fără întârziere, cu privire la orice act legislativ de modificare sau orice modificare ulterioară a acestora.

Articolul 84 - Sancțiuni[92]

(1) Statele membre stabilesc normele privind alte sancțiunile aplicabile în caz de încălcare a prezentului regulament, în special pentru încălcări care nu fac obiectul unor amenzi administrative în temeiul articolului 83, și iau toate măsurile necesare pentru a garanta faptul că acestea sunt puse în aplicare. Sancțiunile respective sunt eficace, proporționale și disuasive.

(2) Fiecare stat membru informează Comisia cu privire la dispozițiile de drept intern pe care le adoptă în temeiul alineatului (1) până la 25 mai 2018, precum și, fără întârziere, cu privire la orice modificare ulterioară a acestora.

Articolul 58 – Competențe ANSPDCP[93]

(1) Fiecare autoritate de supraveghere are toate următoarele competențe de investigare:

(a) de a da dispoziții operatorului și persoanei împuternicite de operator și, după caz, reprezentantului operatorului sau al persoanei împuternicite de operator să furnizeze orice informații pe care autoritatea de supraveghere le solicită în vederea îndeplinirii sarcinilor sale;
(b) de a efectua investigații sub formă de audituri privind protecția datelor;

[91] Art. 58 Regulamentului (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
[92] Art. 84 Regulamentului (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
[93] Art. 58 Regulamentului (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

(c) de a efectua o revizuire a certificărilor acordate în temeiul articolului 42 alineatul (7);
(d) de a notifica operatorul sau persoana împuternicită de operator cu privire la presupusa încălcare a prezentului regulament;
(e) de a obține, din partea operatorului și a persoanei împuternicite de operator, accesul la toate datele cu caracter personal și la toate informațiile necesare pentru îndeplinirea sarcinilor sale;
(f) de a obține accesul la oricare dintre incintele operatorului și ale persoanei împuternicite de operator, inclusiv la orice echipamente și mijloace de prelucrare a datelor, în conformitate cu dreptul Uniunii sau cu dreptul procesual intern.

(2) Fiecare autoritate de supraveghere are toate următoarele competențe corective:

(a) de a emite avertizări în atenția unui operator sau a unei persoane împuternicite de operator cu privire la posibilitatea ca operațiunile de prelucrare prevăzute să încălce dispozițiile prezentului regulament;
(b) de a emite mustrări adresate unui operator sau unei persoane împuternicite de operator în cazul în care operațiunile de prelucrare au încălcat dispozițiile prezentului regulament;
(c) de a da dispoziții operatorului sau persoanei împuternicite de operator să respecte cererile persoanei vizate de a-și exercita drepturile în temeiul prezentului regulament;
(d) de a da dispoziții operatorului sau persoanei împuternicite de operator să asigure conformitatea operațiunilor de prelucrare cu dispozițiile prezentului regulament, specificând, după caz, modalitatea și termenul-limită pentru aceasta;
(e) de a obliga operatorul să informeze persoana vizată cu privire la o încălcare a protecției datelor cu caracter personal;
(f) de a impune o limitare temporară sau definitivă, inclusiv o interdicție asupra prelucrării;
(g) de a dispune rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării, în temeiul articolelor 16, 17 și 18, precum și notificarea acestor acțiuni destinatarilor cărora le-au fost divulgate datele cu caracter personal, în conformitate cu articolul 17 alineatul (2) și cu articolul 19;
(h) de a retrage o certificare sau de a obliga organismul de certificare să retragă o certificare eliberată în temeiul articolul 42 și 43 sau de a obliga organismul de certificare să nu elibereze o certificare în cazul în care cerințele de certificare nu sunt sau nu mai sunt îndeplinite;

(i) de a impune amenzi administrative în conformitate cu articolul 83, în completarea sau în locul măsurilor menționate la prezentul alineat, în funcție de circumstanțele fiecărui caz în parte;
(j) de a dispune suspendarea fluxurilor de date către un destinatar dintr-o țară terță sau către o organizație internațională.

(3) Fiecare autoritate de supraveghere are toate următoarele competențe de autorizare și de consiliere:

(a) de a oferi consiliere operatorului în conformitate cu procedura de consultare prealabilă menționată la articolul 36;

(b) de a emite avize, din proprie inițiativă sau la cerere, parlamentului național, guvernului statului membru sau, în conformitate cu dreptul intern, altor instituții și organisme, precum și publicului, cu privire la orice aspect legat de protecția datelor cu caracter personal;
(c) de a autoriza prelucrarea menționată la articolul 36 alineatul (5), în cazul în care dreptul statului membru prevede o astfel de autorizare prealabilă;
(d) de a emite un aviz și de a aproba proiectele de coduri de conduită, în conformitate cu articolul 40 alineatul (5);
(e) de a acredita organismele de certificare în conformitate cu articolul 43;
(f) de a emite certificări și de a aproba criterii de certificare în conformitate cu articolul 42 alineatul (5);
(g) de a adopta clauzele standard în materie de protecție a datelor menționate la articolul 28 alineatul (8) și la articolul 46 alineatul (2) litera (d);
(h) de a autoriza clauzele contractuale menționate la articolul 46 alineatul (3) litera (a);
(i) de a autoriza acordurile administrative menționate la articolul 46 alineatul (3) litera (b); și de a aproba reguli corporatiste obligatorii în conformitate cu articolul 47.
(4) Exercitarea competențelor conferite autorității de supraveghere în temeiul prezentului articol face obiectul unor garanții adecvate, inclusiv căi de atac judiciare eficiente și procese echitabile, prevăzute în dreptul Uniunii și în dreptul intern în conformitate cu carta.
(5) Fiecare stat membru prevede, pe cale legislativă, faptul că autoritatea sa de supraveghere are competența de a aduce în fața autorităților judiciare cazurile de încălcare a prezentului regulament și, după caz, de a iniția sau de a se implica într-un alt mod în proceduri judiciare, în scopul de a asigura aplicarea dispozițiilor prezentului regulament.
(6) Fiecare stat membru poate să prevadă în dreptul său faptul că autoritatea sa de supraveghere are competențe suplimentare, în afară celor menționate la alineatele (1), (2) și (3). Exercitarea acestor competențe nu afectează modul de operare eficientă a capitolului VII.

MĂSURI CORECTIVE ȘI SANCȚIUNI PREVĂZUTE DE LEGEA 190/2018

LEGE nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi 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 şi de abrogare a Directivei 95/46/CE

Regulamentul general privind protecția datelor la capitolul 1 prin prevederile Art. 1:stabilește măsurile necesare punerii în aplicare la nivel național, în principal, a prevederilor art. 6 alin. (2), art. 9 alin. (4), art. 37-39, 42, 43, art. 83 alin. (7), art. 85 şi ale art. 87-89 din Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal şi libera circulație a acestor date şi de abrogare a Directivei 95/46/CE, publicat în Jurnalul Oficial al Uniunii Europene, seria L, nr. 119 din 4 mai 2016, denumit în continuare Regulamentul general privind protecția datelor.

În aplicarea Regulamentului general privind protecția datelor şi a prezentei legi, termenii şi expresiile de mai jos se definesc după cum urmează: [94]

[94]LEGE nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce

a) autorități și organisme publice -
b) numărul de identificare național ;
c) planul de remediere remediere;
d) măsură de remediere ;
e) termen de remediere

În cuprinsul prezentei legi sunt, de asemenea, aplicabile definițiile prevăzute la art. 4 din Regulamentul general privind protecția datelor.

Reguli speciale privind prelucrarea unor categorii de date cu caracter personal.

Prelucrarea datelor genetice, a datelor biometrice sau a datelor privind sănătatea este reglementata de către articolul 3 din lege. Astfel,

Prelucrarea datelor genetice, biometrice sau a datelor privind sănătatea, în scopul realizării unui proces decizional automatizat sau pentru crearea de profiluri, este permisă cu consimțământul explicit al persoanei vizate sau dacă prelucrarea este efectuată în temeiul unor dispoziții legale exprese, cu instituirea unor măsuri corespunzătoare pentru protejarea drepturilor, libertăților şi intereselor legitime ale persoanei vizate. De asemenea prelucrarea datelor privind sănătatea realizată în scopul asigurării sănătății publice, astfel cum este definită în Regulamentul (CE) nr. 1.338/2008 al Parlamentului European şi al Consiliului din 16 decembrie 2008 privind statisticile comunitare referitoare la sănătatea publică, precum şi la sănătatea şi siguranța la locul de muncă, publicat în Jurnalul Oficial al Uniunii Europene, seria L, nr. 354/70 din 31 decembrie 2008, nu se poate efectua ulterior, în alte scopuri, de către terțe entități.

Prelucrarea unui număr de identificare național [95]

Prelucrarea unui număr de identificare național, inclusiv prin colectarea sau dezvăluirea documentelor ce îl conțin, se poate efectua în situațiile prevăzute de art. 6 alin. (1) din Regulamentul general privind protecția datelor si se efectuează cu instituirea de către operator a următoarelor garanții:

k) punerea în aplicare de măsuri tehnice şi organizatorice adecvate pentru respectarea, în special, a principiului reducerii la minimum a datelor, precum şi pentru asigurarea securității şi confidențialității prelucrărilor de date cu caracter personal, conform dispozițiilor art. 32 din Regulamentul general privind protecția datelor;
l) numirea unui responsabil pentru protecția datelor, în conformitate cu prevederile art. 10 din prezenta lege;
m) stabilirea de termene de stocare în funcție de natura datelor şi scopul prelucrării, precum şi de termene specifice în care datele cu caracter personal trebuie șterse sau revizuite în vederea ștergerii;

privește prelucrarea datelor cu caracter personal şi privind libera circulație a acestor date şi de abrogare a Directivei 95/46/CE

[95] Art 6 LEGE nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal şi privind libera circulație a acestor date şi de abrogare a Directivei 95/46/CE

n) instruirea periodică cu privire la obligațiile ce le revin a persoanelor care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, prelucrează date cu caracter personal.

Referitor la prelucrarea datelor cu caracter personal în contextul relațiilor de muncă, in cazul în care sunt utilizate sisteme de monitorizare prin mijloace de comunicații electronice şi/sau prin mijloace de supraveghere video la locul de muncă, prelucrarea datelor cu caracter personal ale angajaților, în scopul realizării intereselor legitime urmărite de angajator, este permisă numai dacă:

a) interesele legitime urmărite de angajator sunt temeinic justificate şi prevalează asupra intereselor sau drepturilor şi libertăților persoanelor vizate;

b) angajatorul a realizat informarea prealabilă obligatorie, completă şi în mod explicit a angajaților;

c) angajatorul a consultat sindicatul sau, după caz, reprezentanții angajaților înainte de introducerea sistemelor de monitorizare;

d) alte forme şi modalități mai puțin intruzive pentru atingerea scopului urmărit de angajator nu şi-au dovedit anterior eficienta; şi durata de stocare a datelor cu caracter personal este proporțională cu scopul prelucrării, dar nu mai mare de 30 de zile, cu excepțiasituațiilor expres reglementate de lege sau a cazurilor temeinic justificate.

In contextul îndeplinirii unei sarcini care servește unui interes public, prelucrarea datelor personale şi speciale se face conform art. 6 alin. (1) lit. e) şi art. 9 lit. g) din Regulamentul general privind protecția datelor se efectuează cu instituirea de către operator sau de către partea terță a următoarelor garanții:

a) punerea în aplicare a măsurilor tehnice şi organizatorice adecvate pentru respectarea principiilor enumerate la art. 5 din Regulamentul general privind protecția datelor, în special a reducerii la minimum a datelor, respectiv a principiului integrității şi confidențialității;
b) numirea unui responsabil pentru protecția datelor, dacă aceasta este necesară în conformitate cu art. 10 din prezenta lege;
c) stabilirea de termene de stocare în funcție de natura datelor şi scopul prelucrării, precum şi de termene specifice în care datele cu caracter personal trebuie şterse sau revizuite în vederea ştergerii.

Derogări prevăzute de lege.[96]

Prelucrarea datelor cu caracter personal în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare În vederea asigurării unui echilibru între dreptul la protecția datelor cu caracter personal, libertatea de exprimare şi dreptul la informație, prelucrarea în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare poate fi efectuată, dacă aceasta privește date cu caracter personal

[96]LEGE nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal şi privind libera circulație a acestor date şi de abrogare a Directivei 95/46/CE

care au fost făcute publice în mod manifest de către persoana vizată sau care sunt strâns legate de calitatea de persoană publică a persoanei vizate ori de caracterul public al faptelor în care este implicată, prin derogare de la următoarele capitole din Regulamentul general privind protecția datelor: a) capitolul II - Principii; b) capitolul III - Drepturile persoanei vizate; c) capitolul IV - Operatorul şi persoana împuternicită de operator; d) capitolul V - Transferurile de date cu caracter personal către tari terțe sau organizații internaționale; e) capitolul VI - Autorități de supraveghere independente; f) capitolul VII - Cooperare şi coerență; g) capitolul IX - Dispoziții referitoare la situații specifice de prelucrare.

La Capitolul IV legea prevede modalitatea de desemnarea şi sarcinile responsabilului cu protecția datelor.

Astfel operatorii şi persoanele împuternicite de operator desemnează un responsabil cu protecția datelor în situațiile şi condițiile prevăzute la art. 37-39 din Regulamentul general privind protecția datelor, iar in cazul în care operatorul sau persoana împuternicită de operator este o autoritate publică sau un organism public, astfel cum este definit la art. 2 alin. (1) lit. a), poate fi desemnat un responsabil cu protecția datelor, unic pentru mai multe dintre aceste autorități sau organisme, luând în considerare structura organizatorică şi dimensiunea acestora.

De asemenea activitatea şi sarcinile responsabilului cu protecția datelor se realizează cu respectarea prevederilor art. 38 şi 39 din Regulamentul general privind protecția datelor şi a reglementărilor legale naționale aplicabile.

Organisme de certificare[97]

Acreditarea organismelor de certificare

Acreditarea organismelor de certificare prevăzute la art. 43 din Regulamentul general privind protecția datelor se realizează de Asociația de Acreditare din România - RENAR, în calitate de organism național de acreditare, în conformitate cu Regulamentul (CE) nr. 765/2008 al Parlamentului European şi al Consiliului din 9 iulie 2008 de stabilire a cerințelor de acreditare şi de supraveghere a pieței în ceea ce privește comercializarea produselor şi de abrogare a Regulamentului (CEE) nr. 339/93, publicat în Jurnalul Oficial al Uniunii Europene, seria L, nr. 218 din 13 august 2008, precum şi în conformitate cu Ordonanța Guvernului nr. 23/2009 privind activitatea de acreditare a organismelor de evaluare a conformității, aprobată cu modificări prin Legea nr. 256/2011 (2) Organismele de certificare vor fi acreditate potrivit reglementărilor legale aplicabile, în conformitate cu standardul EN-ISO/IEC 17065 şi cu cerințele suplimentare stabilite de Autoritatea națională de supraveghere, precum şi cu respectarea prevederilor art. 43 din Regulamentul general privind protecția datelor.

Măsuri corective şi sancțiuni

[97]LEGE nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal şi privind libera circulație a acestor date şi de abrogare a Directivei 95/46/CE

Dispozițiile generale privind măsuri corective şi sancțiuni privind încălcarea legii sunt prevăzute de capitolul VI din lege.

Astfel:
Încălcarea dispozițiilor enumerate la art. 83 alin. (4)-(6) din Regulamentul general privind protecția datelor constituie contravenție.

Pentru încălcările dispozițiilor următoare, în conformitate cu alineatul (2), se aplică amenzi administrative de până la 10 000 000 EUR sau, în cazul unei întreprinderi, de până la 2 % din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare:

Sancțiunile contravenționale principale sunt avertismentul şi amenda contravențională, iar încălcarea prevederilor art. 3-9 din prezenta lege constituie contravenție şi se sancționează în condițiile prevăzute la art. 83 alin. (5) din Regulamentul general privind protecția datelor.

Constatarea contravențiilor prevăzute de prezenta lege şi aplicarea sancțiunilor contravenționale, precum şi a celorlalte măsuri corective prevăzute de art. 58 din Regulamentul general privind protecția datelor se fac de Autoritatea națională de supraveghere, în conformitate cu dispozițiile Regulamentului general privind protecția datelor, ale Legii nr. 102/2005 privind înființarea, organizarea şi funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările şi completările ulterioare, şi ale prezentei legi.

Aplicarea măsurilor corective autorităților şi organismelor publice [98]

În cazul constatării încălcării prevederilor Regulamentului general privind protecția datelor şi ale prezentei legi de către autoritățile/organismele publice, Autoritatea națională de supraveghere încheie un proces-verbal de constatare şi sancționare a contravenției prin care se aplică sancțiunea avertismentului şi la care anexează un plan de remediere.

Termenul de remediere se stabileşte în funcție de riscurile asociate prelucrării, precum şi demersurile necesar a fi îndeplinite pentru asigurarea conformități prelucrării, iar in termen de 10 zile de la data expirării termenului de remediere, Autoritatea națională de supraveghere poate să reia controlul.

Responsabilitatea îndeplinirii măsurilor de remediere revine autorității/ organismului public care, potrivit legii, poartă răspunderea contravențională pentru faptele constatate.

(5) Modelul planului de remediere care se anexează la procesul-verbal de constatare şi sancționare a contravenției este prevăzut în anexa Plan de remediere, care face parte integrantă din prezenta lege.

[98]LEGE nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal şi privind libera circulație a acestor date şi de abrogare a Directivei 95/46/CE

Cum se face constatarea contravenţiilor şi aplicarea de sancţiuni autorităţilor şi organismelor publice [99]

Dacă în urma controlului prevăzut la art. 13 alin. (3) se constată faptul că autorităţile/organismele publice nu au adus la îndeplinire în totalitate măsurile prevăzute în planul de remediere, Autoritatea naţională de supraveghere, în funcţie de circumstanţele fiecărui caz în parte, poate aplica sancţiunea contravenţională a amenzii, cu luarea în considerare a criteriilor prevăzute la art. 83 alin. (2) din Regulamentul general privind protecţie datelor.

Ce încălcări constituie contravenţii:[100]

Constituie contravenţie încălcarea de către autorităţile/organismele publice a următoarelor dispoziţii din Regulamentul general privind protecţie datelor, referitoare la:

a) obligaţiile operatorului şi ale persoanei împuternicite de operator în conformitate cu prevederile art. 8, art. 11, art. 25-39, art. 42 şi 43;
b) obligaţiile organismului de certificare în conformitate cu art. 42 şi 43;
c) obligaţiile organismului de monitorizare în conformitate cu art. 41 alin. (4).

Constituie contravenţie încălcarea de către autorităţile/organismele publice a dispoziţiilor art. 3-9 din prezenta lege.

Contravenţiile prevăzute la alin. (2) şi (3) se sancţionează cu amendă de la 10.000 lei până la 100.000 lei.

Constituie contravenţie încălcarea de către autorităţile/organismele publice a următoarelor dispoziţii din Regulamentul general privind protecţia datelor, referitoare la:

a) principiile de bază pentru prelucrare, inclusiv condiţiile privind consimţământul, în conformitate cu art. 5-7 şi art. 9;
b) drepturile persoanelor vizate în conformitate cu art. 12-22;
c) transferurile de date cu caracter personal către un destinatar dintr-o ţară terţă sau o organizaţie internaţională, în conformitate cu art. 44-49;
d) orice obligaţii în temeiul legislaţiei naţionale adoptate în temeiul capitolului IX;
e) nerespectarea unei decizii sau a unei limitări temporare sau definitive asupra prelucrării sau a suspendării fluxurilor de date, emisă de către Autoritatea naţională de supraveghere în temeiul art. 58 alin. (2), sau neacordarea accesului, prin încălcarea dispoziţiilor art. 58 alin. (1).

[99]LEGE nr. 190 din 18 iulie 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

[100]LEGE nr. 190 din 18 iulie 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

Prin derogare de la prevederile art. 8 alin. (2) lit. a) din Ordonanța Guvernului nr. 2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări şi completări prin Legea nr. 180/2002, cu modificările şi completările ulterioare, contravențiile prevăzute la alin. (5) se sancționează cu amendă de la 10.000 lei până la 200.000 lei

Constituie contravenție încălcarea de către autoritățile/organismele publice a unei decizii emise de Autoritatea națională de supraveghere în conformitate cu art. 58 alin. (2) coroborat cu art. 83 alin. (2) din Regulamentul general privind protecția datelor.

Prin derogare de la prevederile art. 8 alin. (2) lit. a) din Ordonanța Guvernului nr. 2/2002, cu modificările şi completările ulterioare, contravențiile prevăzute la alin. (7) se sancționează cu amendă de la 10.000 lei până la 200.000 lei.

În aplicarea prevederilor art. 58 alin. (2) lit. b) din Regulamentul general privind protecția datelor, art. 142 alin. (1) din Legea nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, publicată în Monitorul Oficial al României, Partea I, nr. 391 din 9 mai 2005, cu modificările şi completările ulterioare, se modifică şi va avea următorul cuprins:

"Sancțiunile contravenționale principale pe care le aplica Autoritatea națională de supraveghere, potrivit art. 58 alin. (2) lit. b) şi i) din Regulamentul general privind protecția datelor, sunt avertismentul şi amenda. Aplicarea amenzii se face în condițiile art. 83 din Regulamentul general privind protecția datelor."

Bibliografie

Bagnaru, A. M. (2020, 1). Legătura indisolubilă dintre necesitatea de protecţie a datelor cu caracter personal şi rezistenţa la criminalitatea cibernetică. Revista română pentru protecția şi securitatea datelor cu caracter personal, pp. 100-105.

Dumitrescu, M. (2020, 3). Cum pot influenţa standardele ISO/IEC 27001:2013 şi ISO/IEC 27701:2019 procesul de obținere a conformității GDPR. Revista română pentru protecția şi securitatea datelor cu caracter personal, pp. 79-103.

EU Commission. (2018). Ethics and data protection . Brussels: European Commission.

EU Commission. (2016). REGULAMENT nr. 679 din 27 aprilie 2016 privind protecţia datelor cu caracter personal şi privind libera circulaţie a acestor date şi.

ISO/IEC 27701. (2019). Security techniques — Extension to ISO/IEC 27001 and ISO/ IEC 27002 for privacy information management — Requirements and guidelines.

ISO 25010. (2011). Calitatea produselor software.

ISO 27000. (2018). Overview of information security management systems.

Radulescu, M. (2016, Mai). Consideraţii privind selectarea și ierarhizarea soluțiilor de securitate informațională. Audit financiar, pp. 505-515.

PUBLICRESEARCHSRLşiBOCASOFT;Cătălina Giulescu, Cristina Maria Manda, IoanaLefterescu, Carmen Mariana, Dăscălescu Celia Beșciu - Îndrumar metodologic cu tematica prelucrării datelor cu caracter personal în contextul gestionării FESI

Regulamentul (UE) 2016/679

https://www.dataprotection.ro/

https://www.portalprotecțiadatelor.ro/