MANUAL

Modul de formare în domeniul prelucrării datelor cu caracter personal în contextul gestionării FESI

Proiect ”Instruire în domeniul prelucrării datelor cu caracter personal pentru structurile din cadrul sistemului de coordonare, gestionare și control al FESI în România” Cod proiect 3.1.107, Cod SMIS 2014+ 128212

Proiect cofinanțat din Fondul European de Dezvoltare Regională
Programul Operațional Asistență Tehnică 2014-2020

CUPRINS

1. CUVÂNT ÎNAINTE

Prezentul **manual** oferă informații despre protecția datelor cu caracter personal, orientări legale, procedurale și/sau tehnice pentru autoritățile și instituțiile publice, organismele publice/private, specialiștii, beneficiarii sau potențialii beneficiari implicați în gestionarea fondurilor Europene Structurale și de Investiții (FESI). Materialul de față se dorește a fi un instrument aplicabil pentru identificarea modului de asigurare a conformității activităților specifice gestionarii fondurilor FESI prin juxtapunere cu dispozițiile reglementărilor și normelor naționale și europene în domeniul protecției datelor cu caracter personal. Totodată, **manualul** oferă explicații, interpretări, îndrumări și sprijin în aplicarea bunelor practici în materie.

Manualul tratează aspectele teoretice și practice cele mai importante prin prisma prelucrării datelor cu caracter personal și a formelor pe care le îmbracă aceasta în domeniul cu cel mai mare risc, al gestionarii proiectelor finanțate de UE, și prezintă exemple și modele orientative specifice semnificative de protecție din spectrul prelucrării datelor cu caracter personal, încălcărilor principiilor și temeiurilor legale de prelucrare, oferind părților recomandări (inclusiv bune practici) pentru prevenirea, identificarea, și combaterea unor incidente, cu țintă asupra gestionării fondurilor FESI în perioada de programare 2021 – 2027.

Prin examinarea elementelor pe linia prelucrării datelor cu caracter personal **manualul** tratează despre principiile, bunele practici și mecanismele ce trebuie implementate, după caz, la nivel instituțional și/sau la nivel de individ prin considerentele esențiale de educație profesională, etică, morală și integritate, transparență decizională, responsabilitate și responsabilizare.

Manualul ia în considerare prevederi ale convențiilor și reglementarilor juridice în vigoare, deficiențele sistemelor de management și control ca factori de risc majori în generarea și perpetuarea faptelor de încălcare a securității datelor cele mai des întâlnite în domeniul gestionării fondurilor ESI și studii de caz în materie.

Strâns legat de gestionarea proiectelor finanțate de Uniunea Europeana (UE), prin spețele și studiile de caz enunțate și dezbătute, **manualul** reprezintă un instrument practic care își propune să conștientizeze părțile interesate despre tiparele specifice protecției datelor cu caracter personal care pot afecta fondurile UE și, totodată, să îndrume către identificarea șabloanelor, precum și drept material de instruire și de transfer de cunoștințe în prevenirea și înlăturarea cauzelor care conduc la incidente de securitate a datelor în domeniul gestionării fondurilor ESI.

Autorii **manualului** au încredere că informațiile prezentate vor încuraja părțile, fie că este vorba de indivizi, fie că este vorba de autorități publice și entități publice/private, să-și exprime interesul major în implementarea conformității prelucrării datelor cu caracter personal conform legislației naționale și europene în gestionarea fondurilor UE dar și în activitățile conexe publice sau private și să devină pro-activi în identificarea și denunțarea faptelor de încălcare a securității datelor prin poziționarea ferma și fără echivoc împotriva unor astfel de fapte.

INTRODUCERE GENERALĂ

Prezentul manual de curs a fost elaborat în cadrul proiectului „ Instruire în domeniul prelucrării datelor cu caracter personal pentru structurile din cadrul sistemului de coordonare, gestionare și control al FESI în România" – cod proiect 3.1.107, cod SMIS 2014+ 128212, în concordanță cu exigențele legislației europene și naționale pe linia protecției datelor cu caracter personal și este fundamentat pe studiul și analiza unui set de reglementări juridice și documente analitice, de interpretare și orientare, după cum urmează:

1.1 Cadru legislativ european

Legislația europeană identificată ca fiind relevantă:

- **Regulamentul (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/CE (Regulamentul General privind Protecția Datelor – RGPD);
- **Directiva (UE) nr. 680/2016** 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 Uniunii Europene;
- **Directiva 2002/58/CE** privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice);
- **Regulamentul (UE) 2018/1725** al Parlamentului European și al Consiliului din 23 octombrie 2018 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 și de abrogare a Regulamentului (CE) nr. 45/2001și a Deciziei nr. 1247/2002/CE, intrat în vigoare la 11 decembrie 2018.

European Data Protection Board

Comitetul European pentru Protecția Datelor – Recomandări și bune practici în domeniu: https://edpb.europa.eu/our-work-tools/general-guidance/RGPD-guidelines-recommendations-best-practices_ro

1.2 Cadru legislativ național

Legislația națională identificată ca fiind relevantă:

- **Legea nr. 129/2018** pentru modificarea și completarea Legii nr. 102/2005 privind înființarea, organizarea și funcționarea ANSPDCP, precum și pentru abrogarea Legii nr. 677/2001;
- **Legea nr. 190/2018** privind măsuri de punere în aplicare a Regulamentul (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/CE (Regulamentul General privind Protecția Datelor – RGPD);

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal – Legislație, Știri, Recomandări și bune practici în domeniu: https://www.dataprotection.ro/

- **Decizia nr. 99/2018** privind încetarea aplicabilității unor acte normative cu caracter administrativ emise în aplicarea Legii nr. 677/2001;
- **Decizia nr. 128/2018** privind aprobarea formularului tipizat al notificării de încălcare a securității datelor cu caracter personal în conformitate cu prevederile Regulamentului (UE) 2016/679;
- **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. 174/2018** privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal (DPIA).

2. NOȚIUNI INTRODUCTIVE CU PRIVIRE LA DOMENIUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

2.1 Necesitatea adoptării RGPD (UE) nr.679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date. Elementele de noutate aduse de RGPD cu privire la persoanele vizate și la operatorii de date cu caracter personal și persoanele împuternicite de aceștia

Prelucrarea datelor cu caracter personal trebuie să fie în serviciul cetățenilor.

Însă, dreptul la protecția datelor cu caracter personal nu este un drept absolut, ceea ce înseamnă că el 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.

În cursul anului 2012, pe fondul evoluțiilor tehnologice fără precedent, al globalizării și al intensificării substanțiale a fluxurilor transfrontaliere de date cu caracter personal, Comisia Europeană a semnalat necesitatea adaptării corespunzătoare a cadrului juridic european în materia protecției datelor cu caracter personal, propunând noi reguli care să fie statuate în cuprinsul unui regulament adoptat sub egida Parlamentului European și a Consiliului Uniunii Europene.

RGPD (UE) nr. 679 a intrat în vigoare la data de 25 mai 2016, începerea aplicării efective a dispozițiilor sale fiind stabilită pentru 25 mai 2018. El stabilește un set unic și precis de reguli direct aplicabile pe teritoriul tuturor statelor membre UE, în scopul protejării cât mai eficiente a vieții private a persoanelor fizice din întreg spațiul Uniunii. Ca atare, principiile și regulile stabilite de acest nou instrument juridic au o dimensiune specifică, întrucât privesc un drept fundamental al persoanei fizice, anume dreptul la protecția datelor cu caracter personal, garantat prin Carta drepturilor fundamentale a UE (art. 8) și Tratatul de funcționare a UE (art. 16).

RGPD pune un accent deosebit pe **transparența** față de persoana vizată și pe **responsabilizarea** operatorilor de date față de modul în care prelucrează datele cu caracter personal. Sintetizate la maximum, **principalele obligații** ale operatorilor de date în aplicarea RGPD constau în:

a) desemnarea unui responsabil cu protecția datelor;
b) cartografierea (păstrarea evidenței) prelucrărilor de date cu caracter personal;
c) prioritizarea acțiunilor de întreprins în funcție de riscurile pe care le prezintă prelucrările efectuate pentru drepturile și libertățile persoanelor vizate;
d) gestionarea riscurilor pentru drepturile și libertățile persoanelor vizate;
e) organizarea procedurilor interne care să garanteze respectarea protecției datelor în orice moment.

RGPD **consolidează** drepturile garantate persoanelor vizate și **introduce noi drepturi**: dreptul **„de a fi uitat"**, dreptul la **portabilitatea datelor** și dreptul la **restricționarea prelucrării.**

RGPD introduce **sancțiuni severe**, constând în **amenzi administrative** în cuantum de până la 10-20 milioane euro sau între 2-4% din cifra anuală de afaceri la nivel internațional, în cazul operatorilor de date din sectorul privat.

Conform prevederilor RGPD, prin Legea 190/2018 privind măsuri de punere în aplicare a acestuia, au fost făcute precizări cu privire la **cuantumul sancțiunilor**

aplicabile autorităților/organismelor publice din România, sancțiuni care se regăsesc la art.14 din actul normativ menționat.

Totodată, operatorilor de date le este oferită posibilitatea de a interacționa cu o singură autoritate de supraveghere, în regim de **ghișeu unic (one stop shop)**, respectiv cea din statul membru UE în care este stabilit sediul principal al operatorului de date.

Pentru operatorii din România, prin Legea nr. 129/2018 a fost modificată și completată Legea nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal.

Scopul esențial al RGPD este acela de a contribui la asigurarea unei zone de libertate, securitate și justiție în spațiul UE, o zonă în care să fie asigurat atât progresul economic și social, cât și binele individual.

2.2 Obiect și obiective ale reglementării

Atât litera, cât și spiritul RGPD consfințesc un echilibru incontestabil, în vastul și sensibilul domeniu al prelucrării datelor cu caracter personal, între principiul sacrosanct al respectării depline a drepturilor și libertăților fundamentale ale persoanei vizate, pe de o parte, și asigurarea liberei circulații a acestor date, pe de altă parte; totodată, echilibrul și raționalismul noii reglementări europene vizează și armonizarea judicioasă - sub aspectul prevalenței și în raport de importanța valorilor social-economice ocrotite – între interesul public (fie al statelor membre, fie al UE în ansamblul său), interesul legitim al operatorului sau al persoanei împuternicite de operator sau exercițiul autorității publice/unei funcții publice, pe de o parte, și interesul legitim, interesul vital și drepturile și libertățile fundamentale ale persoanelor vizate ori ale altor persoane ce intră, colateral, sub incidența prelucrării datelor cu caracter personal, pe de altă parte.

Sintetizând, RGPD oferă cadrul juridic adecvat atât protecției persoanelor fizice în procesul de prelucrare a datelor cu caracter personal, cât și liberei circulații a acestor date, tratând cu justețe și acuratețe de reglementare două planuri esențiale ale materiei pe care o studiem: a) protecția drepturilor și libertăților fundamentale ale persoanelor fizice, cu accent special asupra datelor cu caracter personal; b) libera circulație a datelor cu caracter personal în interiorul UE, care nu poate fi restricționată sau interzisă din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

Cu alte cuvinte, fie că ne poziționăm în segmentul forței publice al prelucrării datelor cu caracter personal, fie că ne plasăm în perimetrul rezervat persoanei fizice (sub aspectul protecției vieții sale intime și private), suntem guvernați de

principiul „sub lege libertas", adică al libertății care emană strict de la legea interpretată „lato sensu" (fie dreptul intern, fie reglementările europene și/sau internaționale).

2.3 Domeniul de aplicare teritorial a RGPD

Regulile stabilite în cadrul RGPD sunt aplicabile tuturor operatorilor de date, indiferent de locul unde sunt stabiliți aceștia, în anumite condiții bine determinate. Corelativ, RGPD protejează viața privată a tuturor persoanelor fizice vizate aflate pe teritoriul UE, indiferent de cetățenia acestora, ale căror date cu caracter personal sunt prelucrate de persoane fizice sau juridice, autorități publice, agenții sau alte organisme de drept public sau de drept privat.

Astfel, RGPD se aplică:

a) prelucrării datelor cu caracter personal în cadrul activităților derulate la sediul unui operator sau al unei persoane împuternicite de operator pe teritoriul UE, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii;

b) prelucrării datelor cu caracter personal ale unor persoane vizate care se află în UE de către un operator sau persoană împuternicită de operator care nu este stabilit(ă) în Uniune, atunci când activitățile de prelucrare sunt legate de :

- ✓ oferirea de bunuri sau servicii unor astfel de persoane vizate în UE, indiferent dacă se solicită sau nu efectuarea unei plăți de către persoana vizată; importanța, în acest caz, este intenția companiei de a oferi în mod efectiv bunuri și/sau servicii unor astfel de persoane, fapt ce poate fi determinat în urma analizei mai multor factori, cum ar fi: utilizarea limbii oficiale a unui stat membru UE, posibilitatea de a plăti în euro sau în altă monedă oficială a statelor membre ori de a livra produsele comandate pe teritoriul UE precum și orice alte indicii similare; sau
- ✓ monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Uniunii; o asemenea monitorizare presupune, spre exemplu, urmărirea comportamentului în mediul on-line, inclusiv utilizarea unor tehnici ulterioare de prelucrare a datelor, cum ar fi crearea de profiluri (astfel de tehnici sunt folosite pentru a stabili preferințele persoanelor, comportamentele și atitudinile acestora);

Pentru mai multe informații vă rugăm să consultați *"Orientările nr. 3/2018 privind domeniul de aplicare teritorial al RGPD (articolul 3)"*, emise de Comitetul European pentru Protecția Datelor, disponibile în limba română la:

https://edpb.europa.eu/our-work-tools/our-documents/riktlinjer/guidelines-32018-territorial-scope-gdpr-article-3-version_ro

c) prelucrării datelor cu caracter personal de către un operator care nu este stabilit în UE, ci într-un loc în care dreptul intern se aplică în temeiul dreptului internațional public.

2.4 Domeniul de aplicare material a RGPD

RGPD este aplicabil prelucrării datelor cu caracter personal, efectuată total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor.

Cu toate acestea, sunt unele categorii de prelucrări de date exceptate în mod expres de la aplicarea prevederilor RGPD, după cum urmează:

a) cele din cadrul unei activități care nu intră sub incidența dreptului UE;
b) cele efectuate de către statele membre atunci când desfășoară activități ce intră sub incidența reglementărilor din Tratatul de funcționare a UE;
c) cele efectuate de către o persoană fizică în cadrul unei activități exclusiv personale sau strict domestice; astfel de activități sunt unele strict personale, excluzând orice legătură cu profesia sau cu vreo activitate comercială (ex. – corespondența personală prin e-mail sau socializarea în mediul on-line);
d) cele efectuate de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor, sau al executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora; acest tip de prelucrări intră sub incidența aplicării Directivei (UE) nr. 680/2016 a Parlamentului European și a Consiliului Uniunii Europene 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.

3. DEFINIȚII

Pentru a înțelege, interpreta și aplica într-un mod cât mai corect dispozițiile RGPD, atât în litera, cât și în spiritul lor, se cuvine, în mod obligatoriu, însușirea integrală a semnificației unor noțiuni și instituții juridice-cheie, condiție sine-qua-non a transpunerii cu rigurozitate în practică a noii reglementări europene. În cele ce urmează, vom încerca să venim în sprijinul participanților la curs pentru înțelegerea principalelor definiții prevăzute de RGPD în funcție de activitățile care trebuie derulate pe linia îndeplinirii atribuțiilor de coordonare, gestionare și control al FESI, astfel:

- **„date cu caracter personal"** - orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată"); o persoană 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 on-line, sau la unul ori mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

Exemple de date cu caracter personal: În cadrul unui proiect gestionat din fonduri FESI se prelucreza datele beneficiarilor finali ai proiectelor, existând indicatori de atins în acest sens. Unul din indicatori fiind, asistarea a cel putin 100 de persoane cu dizabilități. Pentru fiecare beneficiar final se prelucrează numele, prenumele, starea de sănatate, zona geografică.

- **„prelucrare"** – 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 automate, 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;

Exemple de prelucrare:

- Managementul personalului și administrarea statelor de plată în cadrul: structurilor MIPE, echipelor de proiect, etc.
- Accesarea/consultarea unei baze de date cu persoane de contact care conține date cu caracter personal în cadrul proiectelor;
- Înregistrarea în MYSMIS a tuturor cererilor de finanțare din fonduri FESI;
- Distrugerea unor documente care conțin date cu caracter personal la finalul perioadei de stocare a documentelor proiectelor.

- **„persoană vizată"** – orice persoană fizică în viață, ale cărei date cu caracter personal sunt/au fost prelucrate de un operator sau persoană împuternicită de operator;

  Exemple de persoane vizate:
  - Potențiali angajați (candidați), angajați actuali, foști angajați, angajați temporari din cadrul structurilor MIPE și membri ai familiilor acestora;
  - Reprezentanți ai autorităților/organismelor publice dinafara MIPE, participante în activități de coordonare, gestionare și control al FESI
  - Persoanele care fac parte din echipele de proiect, grupurile țintă ale proiectelor, etc.
- **„operator"** – 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; în cazul în care scopul și mijloacele sunt stabilite prin dreptul UE sau prin dreptul intern,

operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul UE sau în dreptul intern;

Exemple operatori:

- Autorități de management a proiectului din cadrul MIPE;
- Beneficiar al unui Proiect pe fonduri FESI care, stabilește scopurile și mijloacele de prelucrare, parteneri ai beneficiarului proiectului, etc.

➢ **„destinatar"** – persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Sunt însă exceptate, nefiind incluse în categoria destinatarilor, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete potrivit dreptului UE sau dreptului intern; prelucrarea datelor de către autoritățile publice respective este supusă normelor aplicabile în materie de protecție a datelor cu caracter personal, în conformitate cu scopurile prelucrării;

Exemple destinatari:

- Reprezentanți ai autorităților/ organismelor publice dinafara MIPE, participante în activități de coordonare, gestionare și control al FESI
- Comisia Europeană cu ocazia transmiterii Rapoartelor privind stadiul derulării Programelor Operaționale

➢ **„consimțământ"** al persoanei vizate – 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 ce o privesc să fie prelucrate;

➢ **„încălcarea securității datelor cu caracter personal"** – 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, ori la accesul neautorizat la acestea;

Exemple încălcări a securității datelor:

- Pierderea unui laptop pe al cărui hard se află Proiecte finanțate din fonduri FESI care conțin date cu caracter personal ale persoanelor vizate care fac parte din:
  - ✓ Echipe de proiect;
  - ✓ Grupuri țintă
  - ✓ Membri AM
- Utilizarea unor rețele nesecurizate pentru transmiterea unor date cu caracter personal ale personalului care coordonează, gestionează și controlează FESI.

➢ **„autoritate de supraveghere"** – o autoritate independentă instituită de un stat membru UE, responsabilă de monitorizarea aplicării RGPD, în scopul protejării drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea și în vederea facilitării liberei circulații a datelor cu caracter personal în cadrul UE;

Exemplu:
În România avem Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal

- **„procedura"** – prezentarea în scris, a tuturor pașilor ce trebuie urmați, a metodelor de lucru stabilite și a regulilor de aplicat necesare îndeplinirii atribuțiilor și sarcinilor, având în vedere asumarea responsabilităților;
  Exemplu:
  - Un ghid al solicitantului pentru depunere de proiect reprezintă în sine o procedură pe care trebuie să o îndeplinească un beneficiar al proiectului respectiv.
- **„procedură operațională"** – prezentarea formalizată, în scris, a tuturor pașilor ce trebuie urmați, a metodelor de lucru stabilite și a regulilor de aplicat în vederea realizării activității, cu privire la aspectul procesual;
  Exemplu:
  - În vederea depunerii unui proiect pe FESI activitatea începe prin întocmirea și depunerii unei Cereri de Finanțare care, după aprobare se transformă în proiectul preconizat cu respectarea tuturor pașilor stabiliți prin Cererea de Finanțare.
- **„anonimizare"** - prelucrarea datelor cu caracter personal în scopul prevenirii ireversibile a identificării persoanei la care se referă. Datele pot fi considerate anonimizate atunci când nu permit identificarea persoanelor la care se referă, și atunci când nu este posibil ca o persoană să fie identificată din date prin orice prelucrare ulterioară a acelorași date sau prin prelucrarea acelorași date împreună cu alte date disponibile sau susceptibile de a fi disponibile;

***Exemplu**: după finalizarea perioadei de monitorizare a unui proiect, datele beneficiarilor se pot anonimiza, păstrându-se de exemplu doar sumele cheltuite pentru fiecare beneficiar. Una din tehnicile anonimizării poate fi generalizarea sau înlocuirea datelor personale care duc la identificarea persoanei cu serii generice de caractere. Ionescu, Popescu înlocuit cu Nume.*

- **„pseudonimizare"** - 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.

***Exemplu**: în cazul implementării unui proiect pe fonduri FESI se prelucrează datele cu caracter personal ale persoanelor vârstnice asistate medical de un software experimental implementat prin intermediul proiectului. Având în vedere că software-ul analizează starea de sănătate a persoanei permanent și*

înregistrează informații privind anumiți indicatori medicali, sistemul trebuie prevăzut cu mecanisme sporite de securitate având în vedere natura prelucrării. Pentru asigurarea securității se procedează la pseudoanonimizare astfel: combinației de nume, prenume și dată naștere a persoanei i se aplică o semnătură hash care este salvată într-o altă locație/bază de date. În cadrul tabelelor active de monitorizare a stării de sănătate a persoanei toate înregistrările de efectuează pe codul hash creat.

4. CATEGORII DE DATE CU CARACTER PERSONAL

În temeiul dreptului european „datele cu caracter personal", așa cum am menționat la capitolul anterior, sunt definite ca fiind informațiile referitoare la o persoană fizică identificată sau identificabilă, și anume, informații despre o persoană a cărei identitate este fie clară în mod evident, fie poate fi, cel puțin, stabilită prin obținerea unor informații suplimentare.

Definițiile juridice ale datelor cu caracter personal nu clarifică momentul în care o persoană este considerată identificată. Identificarea în mod evident presupune elemente care descriu o persoană într-un mod în care aceasta se poate distinge de toate celelalte persoane și poate fi recunoscută ca persoană fizică.

Exemplu:

Numele unei persoane este un prim element de descriere. Deoarece multe dintre nume nu sunt unice, stabilirea identității unei persoane poate necesita elemente de identificare suplimentare pentru a garanta că o persoană nu este confundată cu altcineva – data și locul nașterii sunt deseori utilizate.

În unele cazuri, alte elemente de identificare pot avea un efect similar ca cel al numelui – în cazul persoanelor publice, este suficient să se facă referire la funcția persoanei (directorul Autorității de Management al POAT).

În sensul aplicabilității legislației europene privind protecția datelor, nu este necesară o identificare de înaltă calitate a persoanelor vizate, este suficient ca persoana în cauză să fie identificabilă. O persoană este considerată identificabilă în cazul în care o parte dintre informații conțin elemente de identificare prin intermediul cărora persoana poate fi identificată direct sau indirect.

4.1 Natura datelor

Orice tip de informații pot fi date cu caracter personal cu condiția ca acestea să facă referire la o persoană.

Exemplu:

Recomandările solicitate experților participanți în cadrul un proiect, reprezintă o evaluare a acelui expert stocată în documentele proiectului și reprezintă date cu caracter personal ale acelui expert.

Deci, datele cu caracter personal includ atât informațiile care aparțin vieții private a unei persoane, precum și informațiile referitoare la viața profesională sau publică a acesteia.

Datele pot fi asociate persoanelor și în cazul în care conținutul informațiilor dezvăluie în mod indirect date despre o persoană.

Exemplificăm:

Identificatori cum ar fi: plăcuțe de înmatriculare a autovehiculelor, IMEI-ul telefoanelor mobile, numărul asigurare socială sau națională, documente de participare la cursuri, referințe, înregistrări video, etc.

4.2 Forma datelor

Forma în care datele cu caracter personal sunt stocate sau utilizate nu este relevantă pentru aplicabilitatea legislației privind protecția datelor. Comunicările scrise sau verbale pot conține date cu caracter personal. Pot de asemenea exista imagini fotografiate, inclusiv înregistrări video. Deci atât informațiile înregistrate pe suport electronic, precum și informațiile pe suport hârtie, pot fi date cu caracter personal.

Exemplu:

În cadrul proiectelor pe FESI regăsim date cu caracter personal pe suport de hârtie și în format electronic, în Rapoartele transmise de beneficiarul fondurilor.

De asemenea cu ocazia diverselor Seminarii, prin prezentarea unor pliante, prin fotografierea și filmarea la locul de desfășurare a acestora, se prelucrează date cu caracter personal ale unor persoane vizate participante care, vor fi păstrate atât pe perioada de derulare a proiectului, cât și o anumită perioadă stabilită de legislație după finalizarea acestuia.

4.3 Categorii speciale de date cu caracter personal

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 și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice.** Interdicția menționată nu este însă operantă în următoarele situații alternative:

a) 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 în ipoteza existenței consimțământului valabil exprimat de persoana vizată;

b) 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;

c) 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;

d) 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;

e) prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;

f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare;

g) 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 fundamentale și a intereselor persoanei vizate;

h) 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;

i) 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;

j) 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 și 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 și libertățile persoanelor vizate. Orice registru cuprinzător al condamnărilor penale se ține numai sub controlul unei autorități de stat.

Ce trebuie să reținem:

În cadrul unor proiecte FESI se promovează egalitatea de gen și egalitatea de șanse pentru persoane cu dizabilități. În aceste situații pe linia prelucrării unor categorii speciale de date cu caracter personal denumite și „date sensibile" trebuie să evaluăm serios nivelul de protecție a acestor date, gradul de diseminare, evaluarea impactului campaniilor și activităților de informare și publicitate pe care le realizează beneficiarii fondurilor.

Aceleași măsuri de protecție trebuie să verificăm și atunci când se alocă fonduri pentru proiecte care au la bază modul de incluziune a persoanelor pe criterii etnice.

4.4 Date anonimizate și pseudonimizate

Ținând cont de principiul limitării duratei de păstrare a datelor, datele ar trebui păstrate pe o perioadă strict necesară atingerii scopului pentru care au fost colectate. Dacă un operator dorește să stocheze date după ce devin perimate și nu mai servesc scopului inițial, acestea trebuie să devină anonime.

4.4.1 Datele anonimizate

Datele devin anonime în cazul în care toate elementele de identificare sunt eliminate dintr-un set de date cu caracter personal. Niciun element nu poate fi lăsat în informațiile care, prin exercitarea unui efort rezonabil, ar putea servi la reidentificarea persoanei vizate.

O soluție eficientă de anonimizare împiedică toate părțile să individualizeze o persoană într-un set de date, să stabilească legături între două înregistrări în cadrul unui set de date (sau între două seturi de date separate) și să deducă orice informații într-un astfel de set de date. Prin urmare, în general, doar eliminarea elementelor de identificare directă nu este suficientă pentru a se garanta faptul că identificarea persoanei vizate nu mai este posibilă. Este necesar să se ia măsuri suplimentare pentru a se preveni identificarea, tot în funcție de contextul și de scopurile prelucrării pentru care sunt destinate datele anonimizate.

Chiar dacă procesul anonimizării poate fi un rezultat al prelucrării datelor cu caracter personal cu scopul de a împiedica în mod ireversibil identificarea persoanei vizate, **nu există standarde prescriptive în legislația UE** și de aceea **pot fi avute în vedere mai multe tehnici de anonimizare**. Datele anonimizate în mod corespunzător oferă garanția protecției persoanei în cauză și nu permit identificarea acesteia.

4.4.2 Datele pseudonimizate

Aceste date nu pot fi echivalate cu informațiile anonimizate, întrucât acestea continuă să permită individualizarea unei persoane vizate și posibilitatea creării de legături între aceasta și diferitele seturi de date.

Pentru mai multe informații vă rugăm să consultați Ghidul – tehnici și bune practici de pseudonimizare, noiembrie 2019, emis de E.N.I.S.A. (Agenția Uniunii Europene pentru Cibersecuritate.

Informațiile personale conțin elemente de identificare, cum ar fi numele, data nașterii, sexul și adresa. Când informațiile personale devin pseudonime, elementele de identificare sunt înlocuite cu un pseudonim.

Pseudonimatul este de natură să permită identificarea și, prin urmare, se încadrează în domeniul de aplicare a regimului juridic de protecție a datelor iar acest aspect este deosebit de relevant în contextul cercetării istorice, statistice sau științifice.

În ceea ce privește procesul de pseudonimizare a datelor se va ține cont de următoarele metode care pot fi adaptate și utilizate de către operatori având în vedere gradul de risc și utilizarea intenționată a datelor, astfel:

- ✓ criptare
- ✓ funcții hash
- ✓ tokenizare

Pentru toate persoanele care nu conțin o cheie de decodificare, datele devenite pseudonime pot fi identificabile cu dificultate, legătura cu o identitate existând sub forma pseudonimului plus cheia de decodificare. Pentru acele persoane care au dreptul să utilizeze cheia de decodare, reidentificarea este posibilă ușor.

Trebuie create garanții speciale împotriva utilizării cheilor de codificare de către persoane neautorizate.

5. PRINCIPIILE PRELUCRĂRII DATELOR CU CARACTER PERSONAL

RGPD consacră următoarele principii ferme, sub auspiciile cărora este concepută prelucrarea datelor cu caracter personal. Principiile trebuie aplicate pentru orice prelucrare, inclusiv în contextul activității FESI:

- **Principiul legalității, echității si transparenței** (datele cu caracter personal sunt prelucrate în mod legal, echitabil și transparent față de persoana vizată);
  Prelucrarea datelor cu caracter personal trebuie efectuată în mod transparent. Autoritățile de management (FESI) au obligația ca operatori de a lua toate măsurile adecvate pentru a informa persoanele vizate care pot fi angajați sau beneficiari – cu privire la modul în care sunt utilizate datele lor cu caracter personal.
  Transparența vizează în primul rând informațiile furnizate persoanei fizice înainte de începerea prelucrării, care ar trebui să fie ușor accesibile persoanelor vizate, precum și la informațiile furnizate persoanelor vizate în urma unei cereri de acces la propriile lor date.
  Operatorii ar trebui să înștiințeze persoanele vizate și publicul larg că vor prelucra datele într-un mod legal și transparent și trebuie să fie în măsură să demonstreze conformitatea operațiunilor de prelucrare cu RGPD. Operațiunile de prelucrare în cadrul FESI nu trebuie efectuate în secret, iar persoanele vizate ar trebui să fie conștiente de riscurile potențiale.
  În plus, operatorii, în măsura în care este posibil, trebuie să acționeze într-un mod care să respecte cu promptitudine voința persoanei vizate, în special atunci când consimțământul acesteia constituie temeiul juridic al prelucrării datelor.
- **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;
  Legitimitatea prelucrării datelor cu caracter personal este strâns legată de scopul prelucrării, care trebuie să fie explicit, determinat și legitim, scopul fiind elementul determinat al prelucrării. În concluzie, nu putem vorbi de o prelucrare legală și legitimă în lipsa unui scop legal și legitim.

Scopul operațiunile de prelucrare a datelor în cadrul FESI este bine determinat însă trebuie evidențiată cu preponderență legitimitatea acestuia caracteristică pe baza căreia să se prelucra date atât în scopul inițial, cât și în scop de prelucrare suplimentar.

- **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. Reducerea la minim a datelor vizează în principal determinarea în concret a categoriilor de date cu caracter personal necesare pentru atingerea scopului urmărit prin prelucrare. Mecanismul este esențial în ceea ce teoreticienii denumesc a fi "protecția persoanei față de prelucrare", reducerea la minim reprezentând chiar esența acestei protecții.
  Prelucrarea datelor cu caracter personal în contextul FESI ar trebui să aibă loc cu respectarea acestui principiu și în limitele impuse de legislația în vigoare. Nu trebuie să exagerăm prin colectarea de date cu caracter personal pentru a demonstra îndeplinirea obiectivului și scopului proiectului. Trebuie să luăm în calcul utilizarea acelor identificatori care pot conduce la stabilirea persoanelor vizate participante în proiecte.
- **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 fără întârziere;
  Respectarea acestui principiu în contextul FESI este determinantă deoarece rezultatul final al proiectelor, care este supus controlului, trebuie să fie cel scontat altfel, proiectul nu mai este eligibil din anumite cauze fapt ce poate conduce la reducerea fondurilor alocate și/sau sancțiuni.
- **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 necesară îndeplinirii 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;
  Prin urmare, stocarea legală a datelor care nu mai sunt necesare se poate realiza, de exemplu, prin anonimizarea acestora însă, pentru domeniul FESI trebuie analizată stocarea fizică și electronică (MYSMIS 2014) în contextul regulamentelor europene aplicabile.
- **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;

În funcție de circumstanțele specifice ale fiecărui caz, măsurile tehnice și organizatorice adecvate ar putea include, de exemplu, pseudonimizarea și criptarea datelor cu caracter personal și/sau testarea și evaluarea periodică a eficacității măsurilor, pentru a asigura faptul că prelucrarea datelor se face în condiții de siguranță.

Operațiunile de prelucrare a datelor în cadrul FESI sunt bine determinate însă, deși este obligatorie asigurarea unei transparențe totale, acestea trebuie să fie protejate mai ales în sensul de a nu fi pierdute sau distruse întrucât, conduc la atingerea obiectivului final al proiectelor.

- **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.

Responsabilitatea în contextul prelucrării datelor cu caracter personal în cadrul FESI, revine în principal AM care, elaborează Ghidul Solicitantului, în care trebuie să se prevadă reguli de respectat pe linia conformării prelucrării datelor cu caracter personal cu dispozițiile RGPD.

6. CRITERII LEGITIME PENTRU PRELUCRAREA DATELOR CU CARACTER PERSONAL

6.1 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, conform Art. 6 din RGPD:

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

b) 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;

c) prelucrarea este necesară în vederea **îndeplinirii unei obligații legale** ce îi revine operatorului;

d) prelucrarea este necesară pentru protejarea **intereselor vitale** ale persoanei vizate sau ale altei persoane fizice;

e) prelucrarea este necesară pentru îndeplinirea unei **sarcini care servește unui interes public** sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;

f) 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 ale persoanei 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 necesară și 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.

Toate aceste aspecte trebuie luate în calcul atunci când prin documentele pe care le elaborăm în contextul FESI, prevedem anumite Reguli pentru acordarea finanțării care, trebuie să fie îndeplinite astfel încât Cererile de finanțare să conțină acțiuni pentru conformitatea operațiunilor de prelucrare a datelor cu caracter personal cu dispozițiile RGPD.

6.2 Consimțământul persoanei vizate pentru prelucrarea datelor cu caracter personal

Dezbatem puțin mai pe larg acest temei legal deoarece, în contextul introducerii în Ghidul Solicitantului a unor informații obligatorii privind Grupurile Țintă relevante pentru acțiunea în care se încadrează un proiect, iar ulterior se impune prelucrarea unor date cu caracter personal ale persoanelor care alcătuiesc acest grup, considerăm că este necesar ca acestuia să i se acorde o atenție deosebită în acțiunile de gestionare și control a proiectului.

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 în 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.

7. OBLIGAȚIILE DE FURNIZARE A INFORMAȚIILOR PRIVIND PROCESAREA DATELOR CU CARACTER PERSONAL

RGPD stabilește în sarcina operatorului obligația de a asigura un înalt nivel de transparență în relația cu persoana vizată. Astfel, operatorul va trebui să ia măsuri adecvate pentru a furniza persoanei vizate orice informații cu privire la cine este operatorul de date, scopul în care îi vor fi prelucrate datele, ce date formează obiectul prelucrării, ce drepturi îi sunt garantate, cum își poate exercita aceste drepturi și cine sunt sau vor fi terții cărora operatorul le va divulga datele, dacă este cazul și în măsura în care acest lucru este posibil.

Totodată, operatorul va face orice comunicări persoanei vizate în legătură cu: dreptul de acces al persoanei vizate; dreptul persoanei vizate la rectificarea și ștergerea datelor; dreptul persoanei vizate la restricționarea prelucrării; obligația operatorului de notificare privind rectificarea și ștergerea datelor cu caracter personal sau restricționarea prelucrării; dreptul persoanei vizate la portabilitatea datelor; dreptul persoanei vizate la opoziție față de prelucrarea datelor, îndeosebi în cazul procesului decizional individual automatizat, inclusiv crearea de profiluri; încălcarea securității datelor cu caracter personal.

Această obligație trebuie respectate și în cadrul activităților specifice FESI, pentru categoriile de persoane vizate ale căror date cu caracter personal sunt prelucrate.

Furnizarea informațiilor și comunicările către persoana vizată se face într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu, în special în cazul informațiilor adresate în mod specific unui minor. Informațiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic. La solicitarea persoanei vizate, informațiile pot fi

furnizate verbal, cu condiția ca identitatea persoanei vizate să fie dovedită prin alte mijloace.

Operatorul facilitează exercitarea de către persoana vizată a drepturilor sus menționate. Totuși, este posibil ca, în anumite cazuri, scopurile pentru care un operator prelucrează date cu caracter personal să nu necesite sau să nu mai necesite identificarea unei persoane vizate de către operator, ceea ce determină ca operatorul să nu aibă obligația de a păstra, obține sau prelucra informații suplimentare pentru a identifica persoana vizată în scopul unic al respectării RGPD. Dacă în astfel de situații operatorul poate demonstra că nu este în măsură să identifice persoana vizată, el o va informa pe aceasta, în măsura în care acest lucru este posibil. În asemenea cazuri, dispozițiile specifice ale RGPD (referitoare la dreptul de acces, la dreptul la rectificare și ștergere, la dreptul la restricționarea prelucrării, la obligația de notificare privind rectificarea și ștergerea datelor cu caracter personal sau restricționarea prelucrării și la dreptul la portabilitatea datelor) nu se aplică, exceptând cazul în care persoana vizată, în scopul exercitării drepturilor enumerate, oferă informații suplimentare de natură a permite identificarea sa.

Operatorul furnizează persoanei vizate informații privind acțiunile întreprinse în urma unei cereri, fără întârzieri nejustificate și în orice caz în cel mult 1 lună de la data primirii cererii. Această perioadă poate fi prelungită cu 2 luni atunci când este necesar, ținându-se seama de complexitatea și numărul cererilor. Operatorul va informa persoana vizată cu privire la orice astfel de prelungire, în termen de 1 lună de la data primirii cererii, indicând și motivele întârzierii. Dacă persoana vizată introduce o cerere în format electronic, informațiile sunt furnizate în format electronic acolo unde este posibil, cu excepția cazului în care persoana vizată solicită un alt format.

În situația în care nu ia măsuri cu privire la cererea persoanei vizate, operatorul o informează pe aceasta, fără întârziere și în termen de cel mult 1 lună de la data primirii cererii, cu privire la motivele pentru care nu ia măsuri și la posibilitatea de a depune o plângere în fața unei autorități de supraveghere și/sau de a introduce o cale de atac judiciară.

Informațiile furnizate persoanei vizate, orice comunicare precum și orice măsuri luate cu privire la drepturile persoanei vizate sunt oferite în regim de gratuitate. Cu toate acestea, în cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, operatorul poate:

a) fie să perceapă o taxă rezonabilă ținând cont de costurile administrative pentru furnizarea informațiilor sau a comunicării ori pentru luarea măsurilor solicitate;
b) fie să refuze să dea curs cererii.În astfel de cazuri, operatorului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii.

Informațiile pot fi furnizate persoanelor vizate în combinație cu pictograme standardizate pentru a oferi într-un mod ușor vizibil, inteligibil și clar lizibil o imagine de ansamblu semnificativă asupra prelucrării avută în vedere. În cazul în care pictogramele sunt prezentate în format electronic, acestea trebuie să poată fi citite automat.

8. DREPTURILE PERSOANELOR VIZATE

RGPD conferă persoanelor vizate următoarele drepturi:

Drept	Art. Regulament	Definitie
Dreptul de a fi informat	Art.13,14	oferă dreptul persoanei vizate de a fi informată cu privire la datele care vor fi colectate, scopul, de către cine, unde vor fi transferate datele.
Dreptul de acces	Art. 15	oferă posibilitatea persoanei vizate de a avea o copie a datelor cu caracter personal pe care o societate le deține și se referă la ea.
Dreptul de rectificare	Art.5(1)(d), 16	oferă posibilitatea persoanei vizate de a solicita corecția sau actualizarea datelor cu caracter personal dacă acestea sunt greșite sau inexacte.
Dreptul la ștergere (dreptul de a fi uitat)	Art. 17	oferă posibilitatea persoanei vizate de a solicita ștergerea datelor sale.
Dreptul de a restricționa prelucrarea	Art. 18	oferă posibilitatea persoanei vizate de a solicita întreruperea prelucrării datelor în cazul în care există motive să se procedeze astfel.
Notificarea destinatarilor privind rectificarea, ștergerea datelor sau restrictionarea prelucrării	Art.19	Obligatia operatorului de a notifica destinatarii referitor la orice rectificare sau ștergere a datelor cu caracter personal sau restricționare a prelucrării efectuate în conformitate cu articolul 16, articolul 17 alineatul (1) și articolul 18, cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate.
Dreptul la portabilitatea datelor	Art. 20	oferă posibilitatea persoanei vizate de a obține datele sale într-un format structurat, utilizat în mod curent și care poate fi citit automat și are dreptul de a transmite aceste date altui operator.
Dreptul de a se opune prelucrării	Art. 21	oferă posibilitatea persoanei vizate de a solicita oprirea prelucrării.
Dreptul de a se opune prelucrării în scopul marketingului direct	Art. 21 (2-3)	oferă posibilitatea persoanei vizate de a solicita oprirea prelucrării
Automatizarea procesului decizional și a profilării	Art. 22	oferă posibilitatea persoanei vizate de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care

		produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă
Dreptul de a își retrage consimtamântul oricând	Art. 7(3)	ofera posibilitatea persoanei vizate de a își retrage consimțământul oricând.
Dreptul de a fi informat cu privire la încălcarea securității datelor	Art. 33	oferă posibilitatea persoanei vizate de a fi informată atunci când încălcarea securității este susceptibilă sa genereze un risc ridicat pentru drepturile și libertățile sale.
Dreptul la o cale de atac judiciară eficientă împotriva unei autorități de supraveghere	Art. 78	oferă fiecărei persoane fizice sau juridice 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.
Dreptul la o cale de atac judiciară eficientă împotriva unui operator sau unei persoane împuternicite de operator	Art. 79	oferă posibilitatea persoanei vizate dreptul de a exercita o cale de atac judiciară eficientă în cazul în care consideră că drepturile de care beneficiază în temeiul GDPR au fost încălcate ca urmare a prelucrării datelor sale cu caracter personal.
Dreptul de a fi reprezentat	Art. 80	ofera posibilitatea persoanei vizate de a mandata un organism, o organizație sau o asociație fără scop lucrativ 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.
Dreptul la despăgubiri	Art. 82	oferă posibilitatea persoanei care a suferit un prejudiciu materiale sau moral ca urmare a unei încălcări a regulamentului RGPD să obțină despăgubiri de la operator sau de la persoana împuternicită de operator pentru prejudiciul suferit.

8.1 Disponibilitatea drepturilor pentru fiecare bază legală a prelucrării

Disponibilitatea drepturilor pentru fiecare bază legală a prelucrării este prezentată în tabelul următor:

Dreptul persoanei vizate	**Baza legală a prelucrării**					
	Consimțământ Art. 6(a)	**Contract Art. 6(b)**	**Obligație legală Art. 6(c)**	**Interes vital Art. 6(d)**	**Interes public Art. 6(e)**	**Interes legitim Art. 6(f)**
Retragerea consimțământului	Da	Nu	Nu	Nu	Nu	Nu
Informare	Da	Da	Da	Da	Da	Da
Acces	Da	Da	Da	Da	Da	Da

Rectificare	Da	Da	Da	Da	Da	Da
Ștergere	Da	Nu	Nu	Nu	Nu	Da
Restricționarea procesării	Da	Da	Da	Da	Da	Da
Portabilitatea datelor	Da	Da	Nu	Nu	Nu	Nu
De a obiecta	N/A	Nu	Nu	Nu	Da	Da
Decizii automatizate și profilare	N/A	Nu	Nu	Da	Da	Da

Nota: Tabelul trebuie să fie utilizat doar ca ghid general. Circumstanțele specifice pot afecta evaluarea cererii.

În cadrul proiectelor finanțate din din fonduri FESI au loc prelucrări de date cu caracter personal ale reprezentaților Structurilor implicate în gestiunea fondurilor, proiectelor, ale reprezentanților Beneficiarilor, angajaților/expertilor Beneficiarilor, ale Beneficiarilor finali. Având în vedere că prelucrările se bazează în principal pe prevederile Art. 6 (b) drepturile pe care le pot exercita persoanele vizate sunt limitate la: Informare, Acces, Rectificare. Portabilitatea datelor este un drept discutabil în acest context deoarece datele nu sunt prelucrate în baza Art. 6 (a) Consimțământ.

! Recomandarea este ca pe orice proiect să se efectueze înainte de implementare o analiză a datelor care se vor prelucra, aplicându-se conceptele de "Privacy by Design and by Default". Suplimentar, pentru orice prelucrare se va identifica baza legală pentru prelucrare conform Art. 6 din RGPD.

În cazul în care o persoană vizată își va exercita unul din drepturile conferite de regulament, plecând de la tabelul de mai sus, se va putea efectua o analiză facilă a cererii.

8.2 Procedura de răspuns la cererile persoanei vizate

Un studiu de caz privind procedura de răspuns la cererile persoanei vizate se regăsește în diagrama de proces următoare:

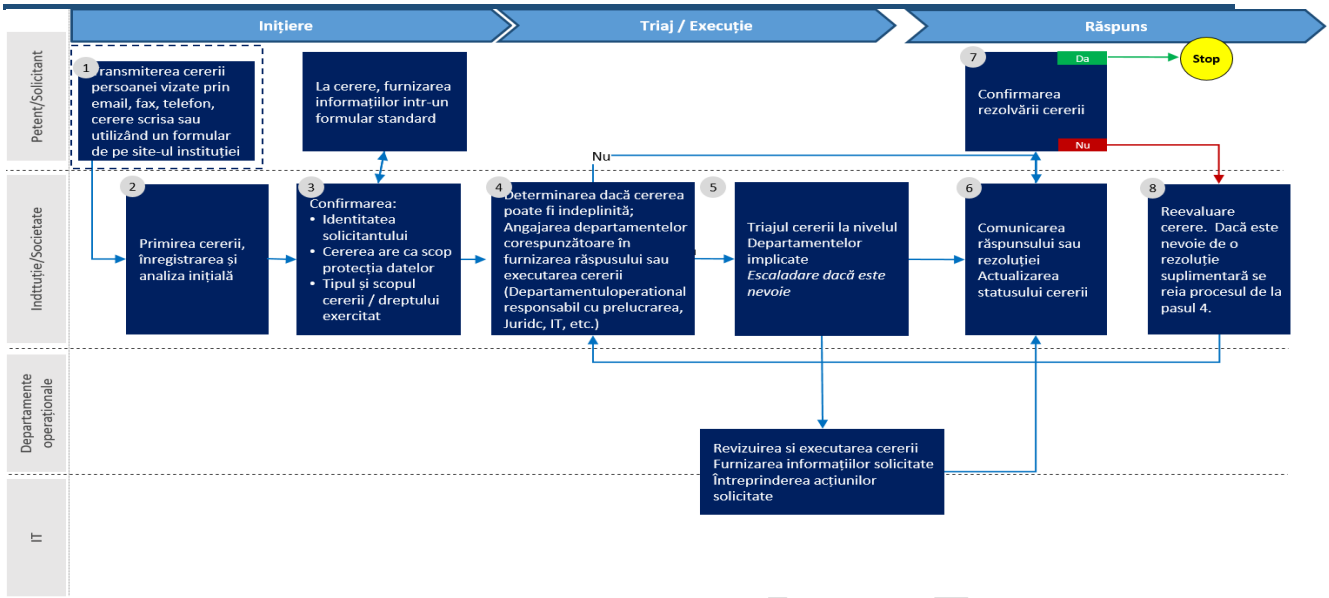


Figura 1. Procedură de răspuns la cererile persoanelor vizate

8.3 Aspecte generale aplicabile oricărei cereri efectuate de persoana vizată

Următoarele aspecte generale se aplică tuturor solicitărilor descrise în acest document și se bazează pe Articolul 12 din GDPR, inclusiv a solicitărilor ce privesc prelucrări de date cu caracter personal efectuate în cadrul activităților de coordonare, implementare și control FESI:

- Trebuie acționat la cererea unei persoane vizate, cu excepția cazului în care nu i se poate stabili identitatea.
- Trebuie furnizate informațiile fără întârzieri nejustificate și în termen de **maxim o lună** de la primirea cererii.
- Informațiile sunt furnizate persoanei vizate într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, folosind un limbaj clar și simplu, în special pentru orice informație adresată în mod specific unui copil.
- Informațiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic. La solicitarea persoanei vizate, informațiile pot fi solicitate și furnizate verbal, cu condiția ca identitatea persoanei vizate să fie dovedită prin alte mijloace.

Atenție! Termenul de răspuns este de maxim 1 lună de la primirea cererii.

Excepțional termenul poate fi prelungit cu două luni – datorită complexității cererii și numarul cererilor!

- Timpul de răspuns poate fi **prelungit cu două luni** atunci când este necesar, ținându-se seama de complexitatea și numărul cererilor. Persoana vizată trebuie informată în termen de o lună de la data solicitării cu privire la prelungirea termenului de răspuns și motivele întârzierii.
- În cazul în care persoana vizată formulează o cerere în format electronic, informațiile sunt furnizate în format electronic acolo unde este posibil, cu excepția cazului în care persoana vizată solicită un alt format.
- În cazul în care se decide că se va da curs unei cereri, persoana vizată trebuie informată fără întârziere și cel târziu în termen de o lună, menționând motivul (motivele), informând în același timp persoana vizată asupra dreptului de a se adresa cu o plângere Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal și/sau de a se adresa instanței de judecată.
- În general, răspunsurile la cereri vor fi acordate gratuit, cu excepția cazului în care acestea sunt "vădit nefondate sau excesive" (în special din cauza caracterului lor repetitiv), caz în care fie se va percepe o remunerație rezonabilă (ținând cont de costurile administrative), fie se va refuza acțiunea. În aceste cazuri, operatorului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii.
- Dacă există îndoieli cu privire la identitatea persoane vizate, se pot solicita informații suplimentare pentru a o stabili.

Notă: Se va solicita persoanelor vizate să furnizeze unul sau două mijloace de identificare, dintre care una trebuie să conțină confirmarea adresei. În cazul în care datele la care se solicită acces includ și fotografia persoanei, în mod obligatoriu se va solicita spre identificare și un mijloc de identificare cu fotografie.

Consultați textul exact al RGPD dacă este necesară clarificarea oricăreia dintre cele de mai sus sau adresați-vă specialistului juridic.

8.4 Descrierea drepturile persoanelor vizate

Drepturile sunt aplicabile tuturor personelor vizate, inclusiv celor ale căror date cu caracter personal se prelucrează în cadrul activităților specifice ale sistemului de coordonare, gestionare și control al FESI.

8.4.1 Dreptul la informare

Persoanele vizate au dreptul de a fi informate cu privire la colectarea şi utilizarea datelor lor personale conform Art. 13 și Art. 14 din RGPD. Aceasta este o cerință esențială de transparență în cadrul RGPD.

Informații care se furnizează în cazul în care datele cu caracter personal sunt colectate de la persoana vizată

În cazul în care datele cu caracter personal referitoare la o persoană vizată sunt colectate de la aceasta, operatorul, în momentul obținerii acestor date cu caracter personal, furnizează persoanei vizate toate informațiile următoare:

a) identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia;
b) datele de contact ale responsabilului cu protecția datelor, după caz;
c) scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;
d) interesele legitime urmărite de operator sau de o parte terță, în cazul în care prelucrarea se efectuează într-un asemenea scop;
e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
f) dacă este cazul, intenția operatorului de a transfera date cu caracter personal către o țară terță sau o organizație internațională și existența sau absența unei decizii a Comisiei Europene privind caracterul adecvat sau, în cazul transferurilor efectuate în baza unor garanții adecvate, a regulilor corporatiste obligatorii ori a unor derogări pentru situații specifice, o trimitere la garanțiile adecvate sau corespunzătoare și la mijloacele de a obține o copie a acestora, în cazul în care acestea au fost puse la dispoziție.

În plus, operatorul mai furnizează persoanei vizate și următoarele informații necesare pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoana vizată:

g) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
h) existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora ori restricționarea prelucrării sau a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;
i) atunci când prelucrarea datelor cu caracter personal, inclusiv a celor din categoriile speciale, are la bază consimțământul explicit al persoanei vizate, existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;
j) dreptul de a depune o plângere în fața unei autorități de supraveghere;
k) dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații;

l) existența unui proces decizional automatizat incluzând crearea de profiluri și referitoare chiar și la prelucrări de categorii speciale de date cu caracter personal, precum și informații pertinente privind logica utilizată, importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată;
m) informații privind scopul secundar al prelucrării și orice informații suplimentare relevante, în ipoteza în care operatorul intenționează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel inițial pentru care acestea au fost colectate.

În cazul în care persoana vizată deține deja informațiile prezentate mai sus, operatorul nu mai are obligația de a i le aduce la cunoștință.

Informații care se furnizează în cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată

În situația în care datele cu caracter personal nu au fost obținute de la persoana vizată, operatorul va furniza persoanei vizate următoarele informații:

a) identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia;
b) datele de contact ale responsabilului cu protecția datelor, după caz;
c) scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;
d) categoriile de date cu caracter personal vizate;
e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz;
f) dacă este cazul, intenția operatorului de a transfera date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională și existența sau absența unei decizii a Comisiei Europene privind caracterul adecvat sau, în cazul transferurilor efectuate în baza unor garanții adecvate, a regulilor corporatiste obligatorii ori a unor derogări pentru situații specifice, o trimitere la garanțiile adecvate sau corespunzătoare și la mijloacele de a obține o copie a acestora, în cazul în care acestea au fost puse la dispoziție.

În mod suplimentar, operatorul mai furnizează persoanei vizate și următoarele informații necesare pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoana vizată, astfel:

g) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili aceasta perioadă;

h) interesele legitime urmărite de operator sau de o parte terță, în cazul în care prelucrarea se efectuează într-un asemenea scop;
i) existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora ori restricționarea prelucrării și a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;
j) atunci când prelucrarea datelor cu caracter personal, inclusiv a celor din categoriile speciale, are la bază consimțământul explicit al persoanei vizate, existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;
k) dreptul de a depune o plângere în fața unei autorități de supraveghere;
l) sursa din care provin datele cu caracter personal și, dacă este cazul, dacă acestea provin din surse disponibile public;
m) existența unui proces decizional automatizat incluzând crearea de profiluri și referitoare chiar și la prelucrări de categorii speciale de date cu caracter personal, precum și informații pertinente privind logica utilizată, importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

Operatorul furnizează toate aceste informații, inclusiv pe cele suplimentare:

- ✓ într-un termen rezonabil după obținerea datelor cu caracter personal, dar nu mai mare de 1 lună, ținându-se seama de circumstanțele specifice în care sunt prelucrate datele cu caracter personal;
- ✓ dacă datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana vizată, cel târziu în momentul primei comunicări către persoana vizată respectivă; sau
- ✓ dacă se intenționează divulgarea datelor cu caracter personal către un alt destinatar, cel mai târziu la data la care acestea sunt divulgate pentru prima oară.

Dacă operatorul intenționează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost obținute, operatorul furnizează persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și orice informații suplimentare relevante, în termenele mai sus menționate.

8.4.2 Dreptul de acces

RGPD permite persoanelor vizate să obțină, din partea operatorului, o confirmare că se prelucrează sau nu date cu caracter personal care le privesc și, în caz afirmativ, acces la datele respective și la alte informații utile.

Art. 15 din RGPR prevede ca persoanei vizate să i se ofere următoarele informații:

a) scopurile prelucrării;
b) categoriile de date cu caracter personal vizate;
c) destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din țări terțe sau organizații internaționale;
d) acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
e) existența dreptului de a solicita operatorului rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării;
f) dreptul de a depune o plângere în fața unei autorități de supraveghere;
g) în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informații disponibile privind sursa acestora;
h) existența unui proces decizional automatizat incluzând crearea de profiluri, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

Ca urmare a dreptului de acces, persoana vizată va primi o informare personalizată, de natură să îi explice informațiile de mai sus, inclusiv dreptul de a depune o plângere la Autoritatea de Supraveghere, dacă nu este mulțumită de modul în care se redactează acest răspuns etc.

În plus față de această informare cu privire la datele prelucrate, persoana vizată are dreptul de a obține o copie a datelor în cauză.

8.4.3 Dreptul la rectificare

Conform Art. 16 din RGPD, persoana vizata are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc. Avându-se în vedere scopurile în care au fost prelucrate datele, persoana vizată are dreptul de a obține completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declarații corespunzătoare.

8.4.4 Dreptul la ștergerea datelor

Persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligația de a șterge datele respective, fără întârzieri nejustificate, în cazul în care este operant unul dintre următoarele motive:

a) datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor în care au fost colectate sau prelucrate;
b) persoana vizată își retrage consimțământul în baza căruia are loc prelucrarea și nu există niciun alt temei juridic pentru prelucrare;
c) persoana vizată se opune prelucrării invocând motive de prevalență a intereselor, drepturilor și libertăților sale în raport cu interesele legitime și imperioase ale operatorului și cu scopul operatorului de constatare, exercitare sau apărare a unui drept al operatorului în instanță, ori persoana vizată se opune prelucrării datelor cu caracter personal ce are drept scop marketingul direct;
d) datele cu caracter personal au fost prelucrate ilegal;
e) datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale care revine operatorului în temeiul dreptului UE sau al dreptului intern sub incidența căruia se află operatorul;
f) datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societății informaționale în mod direct unui minor.

În cazul în care operatorul a făcut publice datele cu caracter personal și este obligat să le șteargă, acesta, ținând cont de tehnologia disponibilă și de costul implementării, va lua măsuri rezonabile, inclusiv de natură tehnică, pentru a informa operatorii care prelucrează datele cu caracter personal că persoana vizată a solicitat ștergerea de către acești operatori a oricăror linkuri către datele respective sau a oricăror copii sau reproduceri ale acestor date cu caracter personal.

Acest drept nu se aplică dacă prelucrarea este necesară:

- ✓ pentru exercitarea dreptului la libera exprimare și la informare;
- ✓ pentru respectarea unei obligații legale care prevede prelucrarea în temeiul dreptului UE sau al dreptului intern ce se aplică operatorului sau pentru îndeplinirea unei sarcini executate în interes public ori în cadrul exercitării unei autorități oficiale cu care este învestit operatorul;
- ✓ din motive de interes public în domeniul sănătății publice;
- ✓ în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în măsura în care exercitarea dreptului la ștergerea datelor este susceptibilă să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective; sau
- ✓ pentru constatarea, exercitarea sau apărarea unui drept în instanță.

8.4.5 Dreptul la restricționarea prelucrării

Dreptul la restricționarea datelor este un drept cu caracter temporar. În unele situații, între momentul în care, spre exemplu, operatorul ia decizia de a șterge anumite date (nu mai are nevoie de datele cu caracter personal în scopul prelucrării) și ștergerea efectivă a datelor dar, persoana vizată face o cerere prin

care se opune ștergerii, motivând faptul că i le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanță. Ca urmare a unei astfel de solicitări, operatorul stopează prelucrarea datelor pentru o anumită perioadă de timp.

În momentul ridicării restricției de prelucrare, Operatorul trebuie să informeze persoana vizată cu privire la faptul că s-a ridicat restricția.

8.4.6 Obligația operatorului de notificare privind rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării acestora

Operatorul comunică fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal orice rectificare sau ștergere a acestor date sau restricționare a prelucrării, cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate. Operatorul are obligația de a informa persoana vizată cu privire la destinatarii respectivi, la solicitarea acesteia.

8.4.7 Dreptul la portabilitatea datelor

Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc și pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent și care poate fi citit automat și are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal. Cu alte cuvinte, datele personale trebuie să poată fi oferite persoanei vizate, într-un format structurat, pentru ca acesta să poată decide că le descarcă sau, dimpotrivă, că le poate trimite unui alt operator.

Acest drept se aplică doar în măsura în care datele sunt prelucrate în temeiul unui contract sau al consimțământului persoanei vizate, precum și (cumulat) atunci când prelucrarea se face prin mijloace automate.

Dreptul la portabilitatea datelor se aplică doar asupra datelor furnizate direct de persoana vizată. Sunt excluse de la portabilitate datele derivate sau deduse, așa cum sunt denumite, de regulă, concluziile pe care le trag operatorii (pe baza unor operațiuni de profilare, de regulă) cu privire la persoanele vizate.

8.4.8 Dreptul la opoziție

Referitor la dreptul la opoziție, RGPD prevede că în orice moment, persoana vizată are dreptul de a se opune prelucrării, din motive legate de situația particulară în care se află și ținând de legalitatea prelucrării datelor cu caracter personal care o privesc, inclusiv creării de profiluri. Operatorul nu va mai prelucra datele cu caracter personal, cu excepția cazului în care acesta demonstrează că are motive legitime și imperioase care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau că scopul prelucrării îl reprezintă constatarea, exercitarea sau apărarea unui drept în instanță.

Atunci când prelucrarea datelor cu caracter personal are drept scop marketingul direct, persoana vizată are dreptul de a se opune în orice moment prelucrării în acest scop a datelor cu caracter personal care o privesc, inclusiv creării de profiluri, în măsura în care este legată de marketingul direct respectiv. În cazul în care persoana vizată se opune prelucrării în scopul marketingului direct, datele cu caracter personal nu mai sunt prelucrate în acest scop.

Dreptul la opoziție față de prelucrarea datelor cu caracter personal în situațiile prezentate mai sus este adus în mod explicit în atenția persoanei vizate de către operator cel târziu în momentul primei comunicări cu aceasta și este prezentat în mod clar și separat de orice alte informații.

În contextul utilizării serviciilor societății informaționale, persoana vizată își poate exercita dreptul de a se opune prin mijloace automate care utilizează specificații tehnice.

În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare științifică sau istorică ori în scopuri statistice, persoana vizată, din motive legate de situația sa particulară, are dreptul de a se opune prelucrării datelor cu caracter personal care o privesc, cu excepția situației în care prelucrarea este necesară pentru îndeplinirea unei sarcini din motive de interes public.

8.4.9 Procesul decizional individual automatizat, inclusiv crearea de profiluri

În ceea ce privește procesul decizional individual automatizat (inclusiv crearea de profiluri), RGPD conferă, în mod expres, persoanei vizate dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice ce privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă.

Exercitarea acestui drept de către persoana vizată nu este operantă în cazul în care decizia respectivă:

a) este necesară pentru încheierea sau executarea unui contract între persoana vizată și un operator de date cu caracter personal;
b) este autorizată prin dreptul UE sau dreptul intern care se aplică operatorului și care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate; sau
c) are la bază consimțământul explicit al persoanei vizate.

În cazurile menționate la literele a) și c), operatorul de date pune în aplicare măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate, cel puțin dreptul acesteia de a obține intervenția umană din partea operatorului, de a-și exprima punctul de vedere și de a contesta decizia respectivă de prelucrare.

Deciziile de acest tip nu au la bază categoriile speciale de date cu caracter personal, cu excepția cazurilor în care:

- ✓ persoana vizată și-a dat consimțământul explicit pentru prelucrarea unor astfel de date în unul sau mai multe scopuri specifice, exceptând situația în care dreptul UE sau dreptul intern prevede că interdicția de prelucrare nu poate fi ridicată prin consimțământul persoanei vizate;
- ✓ 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 fundamentale și a intereselor persoanei vizate.

8.4.10 Dreptul la exercitarea căilor de atac și dreptul la despăgubiri

Dreptul de a depune o plângere la o autoritate de supraveghere

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 regim de competență teritorială alternativă, în special în statul membru UE 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 RGPD.

Autoritatea de supraveghere la care s-a depus plângerea îl informează pe reclamant cu privire la evoluția și rezultatul soluționării plângerii, inclusiv referitor la posibilitatea de a exercita o cale de atac judiciară.

Dreptul la o cale de atac judiciară eficientă împotriva unei autorități de supraveghere

Fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare, 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.

De asemenea, 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 (fie că este vorba despre autoritatea vizată, fie despre autoritatea principală) nu tratează o plângere sau nu informează persoana vizată în termen de 3 luni cu privire la progresele sau la soluționarea plângerii la care ne-am referit mai sus.

Acțiunile introduse împotriva unei autorități de supraveghere sunt aduse în fața instanțelor din statul membru UE în care este stabilită autoritatea de supraveghere.

În 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 European pentru Protecția Datelor în cadrul mecanismului pentru asigurarea coerenței, autoritatea de supraveghere este obligată să transmită instanței avizul respectiv sau decizia respectivă.

Dreptul la o cale de atac judiciară eficientă împotriva unui operator sau unei persoane împuternicite de operator

Fără a aduce atingere vreunei căi de atac administrative sau nejudiciare disponibile, inclusiv dreptului de a depune o plângere la o autoritate de supraveghere competentă, 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 RGPD au fost încălcate ca urmare a prelucrării datelor sale cu caracter personal cu nerespectarea dispozițiilor RGPD.

Acțiunile judiciare introduse împotriva unui operator sau unei persoane împuternicite de operator sunt prezentate în fața instanțelor din statul membru UE unde operatorul sau persoana împuternicită de operator își are un sediu. În mod alternativ, o astfel de acțiune poate fi prezentată în fața instanțelor din statul membru UE 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 la reprezentare în exercitarea căilor de atac

Persoana vizată are dreptul de a 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 la căile de atac administrative și judiciare specifice (depunerea plângerii la o autoritate de supraveghere, exercitarea căii de atac judiciare eficiente împotriva unei autorități de supraveghere și exercitarea căii de atac judiciare eficiente împotriva unui operator sau unei persoane împuternicite de operator), precum și să exercite dreptul de a primi despăgubiri în numele persoanei vizate, dacă acest lucru este prevăzut în dreptul intern.

Dreptul la despăgubiri

Orice persoană care a suferit un prejudiciu material sau moral ca urmare a unei încălcări a dispozițiilor RGPD are dreptul să obțină despăgubiri de la operator sau de la persoana împuternicită de operator pentru prejudiciul suferit.

Orice operator implicat în operațiunile de prelucrare este răspunzător pentru prejudiciul cauzat de operațiunile sale de prelucrare care contravin normelor RGPD.

Persoana împuternicită de operator este răspunzătoare pentru prejudiciul cauzat de prelucrare numai în cazul în care nu a respectat obligațiile prevăzute în RGPD ce revin în mod specific persoanelor împuternicite de operator sau a acționat în afara sau în contradicție cu instrucțiunile legale ale operatorului.

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

În cazul în care mai mulți operatori sau mai multe persoane împuternicite de operator, sau un operator și o persoană împuternicită de operator sunt implicați (implicate) în aceeași operațiune de prelucrare și răspund pentru orice prejudiciu cauzat de prelucrare, fiecare operator sau persoană împuternicită de operator este răspunzător (răspunzătoare) pentru întregul prejudiciu în vederea asigurării despăgubirii efective a persoanei vizate. În situația în care un operator sau o persoană împuternicită de operator a plătit în totalitate despăgubirile pentru prejudiciul creat, respectivul operator sau respectiva persoană împuternicită de operator are dreptul să solicite – pe calea unei acțiuni civile în regres - de la ceilalți operatori sau celelalte persoane împuternicite de operator implicate în aceeași operațiune de prelucrare recuperarea acelei părți din despăgubiri care corespunde părții lor de răspundere pentru prejudiciu.

Acțiunile în exercitarea dreptului de recuperare a despăgubirilor plătite se introduc la instanțele din statul membru UE unde operatorul sau persoana împuternicită de operator își are un sediu. În mod alternativ, o astfel de acțiune poate fi prezentată instanțelor din statul membru UE 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.

9. ETAPELE CONFORMĂRII CU PREVEDERILE RGPD

9.1 Numirea unui Responsabil cu protecția datelor (DPO)

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

RGPD menționează, în cadrul considerentului (97), că în cazul în care prelucrarea este efectuată de o autoritate publică, cu excepția instanțelor sau a autorităților judiciare independente atunci când acționează în calitatea lor judiciară, în cazul în care, în sectorul privat, prelucrarea este efectuată de un operator a cărui activitate principală constă în operațiuni de prelucrare care necesită o monitorizare regulată și sistematică a persoanelor vizate pe scară largă, precum și în situația în care activitatea principală a operatorului sau a persoanei împuternicite de operator constă în prelucrarea pe scară largă de categorii speciale de date cu caracter

personal și de date privind condamnările penale și infracțiunile, **o persoană** care deține cunoștințe de specialitate în materie de legislație și practici privind protecția datelor **ar trebui să acorde asistență** operatorului sau persoanei împuternicite de operator **pentru monitorizarea conformității**, la nivel intern, **cu dispozițiile RGPD**. În sectorul privat, activitățile principale ale unui operator se referă la activitățile sale de bază, și nu la prelucrarea datelor cu caracter personal drept activități auxiliare. Nivelul necesar al cunoștințelor de specialitate ar trebui să fie stabilit în special în funcție de operațiunile de prelucrare a datelor efectuate și de nivelul de protecție impus pentru datele cu caracter personal prelucrate de operator sau de persoana împuternicită de operator. Acești responsabili cu protecția datelor, indiferent dacă sunt sau nu angajați ai operatorului, ar trebui să fie in măsură să își îndeplinească atribuțiile și sarcinile în mod independent.

Desemnarea unui responsabil cu protecția datelor este obligatorie, cu începere din data de 25 mai 2018, date fiind dispozițiile art. 37-39 din RGPD, în cazul în care operatorul sau persoana împuternicită de operator:

- este o autoritate publică sau un organism public, cu excepția instanțelor în exercitarea funcției lor jurisdicționale;
- desfășoară o activitate principală care conduce la realizarea unei monitorizări constante și sistematice pe scară largă a persoanelor vizate;
- desfășoară o activitate principală care constă în supravegherea pe scară largă de date sensibile (cum ar fi: date privind originea rasială sau etnică, convingerile religioase, apartenența sindicală, date genetice, biometrice, privind starea de sănătate) sau referitoare la condamnări penale și infracțiuni.

Chiar dacă entitatea nu are obligația expresă de a desemna un responsabil cu protecția datelor, este recomandabilă și constituie o bună practică numirea acestuia, în considerarea efectului benefic al activității responsabilului pe linia asigurării respectării RGPD de către operatorul respectiv sau persoana împuternicită de operator.

Pentru desemnarea unui responsabil cu protecția datelor operatorul de date trebuie să parcurgă următorii pași:

- stabilirea criteriilor pentru alegerea persoanei care să ocupe poziția de DPO intern, conform recomandărilor din ANEXA 1;
- elaborarea fișei postului prin care se stabilesc atribuțiile DPO, conform modelului orientativ din ANEXA 2;
- emiterea deciziei de numire a DPO;
- alocarea resurselor necesare desfășurării activității (ex: birou, PC, imprimantă, scaner, telefon, etc.);

- declararea DPO la ANSPDCP (prin completarea formularului on-line existent pe site-ul acesteia) și comunicarea internă a datelor de contact ale acestuia;
- elaborarea procedurii de lucru cu DPO, conform modelului orientativ din ANEXA 3;

9.2 Elaborare și implementare documentații

9.2.1 Evidența activităților de prelucrare a datelor aflate în responsabilitatea Operatorului

RGPD statuează în cadrul considerentului (82) faptul că, în vederea demonstrării conformității cu dispozițiile sale, operatorul sau persoana împuternicită de operator ar trebui să păstreze evidențe ale activităților de prelucrare aflate în responsabilitatea sa și să aibă obligația de a coopera cu autoritatea de supraveghere, punând la dispoziția acesteia, la cerere, aceste evidențe, pentru a putea fi utilizate în scopul monitorizării respectivelor operațiuni de prelucrare.

Astfel, potrivit dispozițiilor art. 30 din RGPD, toți operatorii din sistemul public, persoanele împuternicite de operator, precum și operatorii din sistemul privat cu peste 250 de angajați, au obligația cartografierii prelucrării datelor cu caracter personal efectuate. Chiar și operatorii din sistemul privat cu mai puțin de 250 de angajați au obligația cartografierii prelucrărilor în cazurile în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, în situația în care prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date ori date cu caracter personal referitoare la condamnări penale și infracțiuni.

În acest sens, pentru a evalua în mod corect și eficient impactul RGPD asupra activității entității, este necesară identificarea prelucrărilor de date cu caracter personal efectuate (Inventarul) și păstrarea evidenței activităților de prelucrare (Registrul):

a) **Inventarul prelucrărilor de date cu caracter personal**

Acest document va trebui să acopere toate procesele și sub-procesele din cadrul structurilor organizatorice ale unei entități, unde sunt identificate prelucrări de date cu caracter personal. Mai concret, acesta acoperă structurile și procesele importante ale entității și pentru că unele procese sunt interdepartamentale, va fi nominalizat un proprietar al procesului, pentru a desemna o persoană cu autoritatea și responsabilitatea procesului.

- Explicații privind modul în care se completează documentul în format EXCEL se regăsesc în ANEXA 4
- Formatul documentului în EXCEL se regăsește în ANEXA 18

b) **Registrul evidență activități de prelucrare**

După inventarierea realizată, evidența prelucrării datelor cu caracter personal care trebuie păstrată de operator în condițiile stabilite de RGPD, trebuie să cuprindă:

- ✓ numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;
- ✓ scopurile prelucrării;
- ✓ o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;
- ✓ categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale;
- ✓ dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, în cazul transferurilor speciale (altele decât în temeiul unei decizii privind caracterul adecvat al nivelului de protecție, sau în baza unor garanții adecvate, sau în temeiul unor reguli corporatiste obligatorii, ori cărora nu le este aplicabilă vreuna dintre derogările pentru situații specifice), documentația care dovedește existența unor garanții adecvate;
- ✓ acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;
- ✓ acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate (pseudonimizarea și criptarea datelor cu caracter personal; capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare; 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; un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării).

Prin urmare, pentru fiecare prelucrare de date cu caracter personal, este necesar a se avea în vedere următoarele aspecte:

- ❖ **CINE ?**

Se înscriu în evidență numele și coordonatele operatorului (și ale reprezentantului său legal) și, după caz, ale responsabilului cu protecția datelor;

Se întocmește lista persoanelor împuternicite, după caz.

- ❖ **CE ?**

Sunt identificate categoriile de date cu caracter personal prelucrate;

Sunt identificate datele susceptibile de a prezenta riscuri datorită naturii lor sensibile deosebite (datele privind sănătatea sau infracțiunile).

- **DE CE ?**

Se precizează scopul sau scopurile în care sunt colectate sau prelucrate datele cu caracter personal (ex. – gestionarea relației comerciale, managementul resurselor umane, geo localizare, video supraveghere etc.).

- **UNDE ?**

Se stabilește locația sistemului de evidență și, dacă este cazul, se stabilesc și destinatarii datelor.

Se stabilesc statele către care sunt, eventual, transferate datele.

- **PÂNĂ CÂND ?**

Se precizează, pentru fiecare categorie de date, perioada de stocare.

- **CUM ?**

Se precizează măsurile de securitate implementate pentru a reduce la minimum riscurile de acces neautorizat la date și, în consecință, impactul asupra vieții private a persoanelor vizate.

- Formatul documentului în EXCEL se regăsește în ANEXA 19

9.3 Evaluarea impactului asupra protecției datelor - DPIA

În cadrul considerentelor (84) si (94), RGPD menționează că în cazurile în care operațiunile de prelucrare sunt susceptibile să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul trebuie să fie responsabil de efectuarea unei evaluări a impactului asupra protecției datelor, care să estimeze, în special, originea, natura, specificitatea și gravitatea acestui risc. Rezultatul evaluării va trebui luat în considerare la stabilirea măsurilor adecvate menite a demonstra că prelucrarea datelor cu caracter personal este conformă cu dispozițiile RGPD. În cazul în care o evaluare a impactului asupra protecției datelor arată că operațiunile de prelucrare implică un risc ridicat, pe care operatorul nu îl poate atenua prin măsuri adecvate sub aspectul tehnologiei disponibile și al costurilor implementării, ar trebui să aibă loc o consultare prealabilă a autorității de supraveghere înainte de prelucrare.

Un astfel de risc ridicat este susceptibil să fie generat de anumite tipuri de prelucrare, precum și de amploarea și frecvența prelucrării, care pot duce și la producerea unor prejudicii sau pot atinge drepturile și libertățile persoanelor fizice. Autoritatea de supraveghere va trebui să răspundă la cererea de consultare într-un anumit termen. Cu toate acestea, lipsa unei reacții din partea autorității de supraveghere în termenul respectiv ar trebui să nu aducă atingere niciunei intervenții a autorității de supraveghere în conformitate cu sarcinile și competențele sale, inclusiv competența de a interzice operațiuni de prelucrare. Ca urmare a acestui proces de consultare, rezultatul unei evaluări a impactului asupra protecției datelor efectuate cu privire la prelucrarea în cauză poate fi transmis autorității de supraveghere, în special măsurile avute în vedere pentru a atenua riscul asupra drepturilor și libertăților persoanelor fizice.

Art. 35 din RGPD întărește conținutul celor două considerente menționate, stipulând că în cazul în care au fost identificate prelucrări de date cu caracter personal susceptibile de a prezenta riscuri ridicate pentru drepturile și libertățile peroanelor fizice, operatorul va efectua o evaluare a impactului asupra protecției datelor. Evaluarea se realizează anterior colectării datelor cu caracter personal și efectuării prelucrării.

Evaluarea impactului asupra protecției datelor **presupune:**

- ✓ o descriere a prelucrării de date efectuate și a scopurilor acesteia;
- ✓ o evaluare a necesității și a proporționalității prelucrării de date efectuate;
- ✓ o estimare a riscurilor asupra drepturilor și libertăților persoanelor vizate;
- ✓ măsurile prevăzute pentru a trata riscurile și a asigura conformitatea cu dispozițiile RGPD.

Evaluarea impactului asupra protecției datelor **permite**:

- ✓ realizarea unei prelucrări de date cu caracter personal sau a unui produs care respectă viața privată;
- ✓ estimarea impactului asupra vieții private a persoanelor vizate;
- ✓ demonstrarea faptului că principiile fundamentale ale RGPD sunt respectate.

Evaluarea impactului asupra protecției datelor **se impune, în special**, în cazul:

- ✓ 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 ce produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;
- ✓ prelucrării pe scară largă a unor categorii speciale de date sau a unor date cu caracter personal privind condamnări penale și infracțiuni; sau
- ✓ unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.

Evaluarea impactului se poate referi doar la o singură operațiune de prelucrare dar poate fi folosită și pentru a permite estimarea unor multiple operațiuni de prelucrare similare în ceea ce privește natura, obiectivul, contextul și scopul. Într-adevăr, evaluarea impactului urmărește să studieze în mod sistematic situații noi care ar putea conduce la riscuri ridicate pentru drepturile și libertățile persoanelor fizice, astfel încât nu suntem în prezența unei evaluări a impactului în cazurile care deja au fost studiate (adică operațiunile de prelucrare efectuate într-un context specific și pentru un anumit scop). Acest lucru ar putea evidenția situația în care se utilizează o tehnologie similară pentru a colecta același tip de date în aceleași scopuri, dar poate fi aplicabil și operațiunilor de prelucrare similare implementate de diverși operatori de date.

În situația in care operațiunea de prelucrare implică operatori asociați, aceștia trebuie să-și definească în mod precis obligațiile. Evaluarea impactului trebuie să stabilească partea responsabilă pentru diferitele măsuri destinate să trateze riscurile și să protejeze drepturile și libertățile persoanelor vizate. Fiecare operator de date ar trebui să-și exprime nevoile și să împărtășească informații utile fără a compromite secretele (ex. – protecția secretelor comerciale, a proprietății intelectuale, a informațiilor comerciale) sau a dezvălui vulnerabilități.

Pentru a oferi un set mai precis de operațiuni de prelucrare care necesită o evaluare a impactului datorită riscului inerent, în conformitate cu considerentele și dispozițiile RGPD, vor trebui luate în considerare următoarele 9 criterii:

- **Evaluarea sau scoring-ul**, inclusiv profilarea și preconizarea, în special din aspecte privind performanța persoanei vizate la locul de muncă, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările. Asemenea exemple pot include o instituție financiară care își monitorizează clienții într-o bază de date de tip credit sau printr-o bază de date destinată combaterii spălării banilor sau finanțării de acțiuni teroriste ori a unei baze de date constituită împotriva fraudei sau o companie de biotehnologie care oferă teste genetice direct consumatorilor pentru a evalua și previziona riscurile de boală/sănătate ori pentru a crea un profil de comportament sau de marketing bazat pe utilizarea sau navigarea pe site-ul său de web.
- **Proces decizional automatizat cu efecte legale sau similare semnificative** – prelucrare care vizează luarea deciziilor asupra persoanelor vizate, ce produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă (ex. – prelucrarea poate conduce la excluderea sau discriminarea persoanelor). Prelucrarea cu efect redus sau fără efect asupra persoanelor nu corespunde acestui criteriu specific.
- **Monitorizare sistematica** – prelucrare folosită pentru a observa, monitoriza sau controla persoanele vizate, incluzând colectarea de date prin rețele sau monitorizarea sistematică a unei zone accesibile publicului. Acest tip de monitorizare reprezintă un criteriu deoarece datele cu caracter personal pot

fi colectate în situații în care persoanele vizate să nu fie conștiente de cine colectează datele și modul în care acestea vor fi utilizate. În plus, poate fi imposibil ca persoanele să nu fie supuse unei astfel de prelucrări în spațiul (sau zonele publice) accesibile publicului.

- **Date sensibile sau date de natură foarte personală** – includ categoriile de date speciale cu caracter personal și date cu caracter personal privind condamnările penale sau infracțiunile (ex. – un spital general care păstrează dosarele medicale ale pacienților sau un anchetator privat care păstrează detalii privitoare la infractori). Aceste date cu caracter personal sunt considerate ca fiind date sensibile, dincolo de înțelesul obișnuit al termenului, deoarece sunt legate de activitățile casnice și private (ex. – comunicațiile electronice, a căror confidențialitate ar trebui protejată) sau deoarece respectivele date influențează exercitarea unui drept fundamental (ex. – datele de localizare, a căror colectare pune la îndoială libertatea de mișcare) ori pentru că încălcarea lor implică în mod clar efecte grave asupra vieții cotidiene a persoanei vizate (ex. – datele financiare care ar putea fi folosite pentru fraudarea plăților). În acest sens, ar putea fi relevant dacă datele au fost deja puse la dispoziția publicului de către persoana vizată sau de către terți. Faptul că datele cu caracter personal sunt disponibile în mod public poate fi considerat un factor în evaluarea dacă datele se preconizează a fi utilizate în continuare în anumite scopuri. Acest criteriu poate include, de asemenea, datele cuprinse în documente personale, e-mail-urile, jurnalele, notele de la cititorii electronici echipate cu funcții de notare și informații foarte personale conținute în aplicațiile de log.
- **Date prelucrate pe scară largă**, care, în lipsa unei definiții exprese oferită de RGPD, pot fi determinate pe baza unor factori precum: numărul persoanelor vizate, ori un număr exact sau un procent din populația relevantă; volumul datelor și/sau gama de elemente diferite de date aflate în curs de prelucrare; durata sau permanența activității de prelucrare a datelor; suprafața geografică a activității de prelucrare.
- **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 depăși așteptările rezonabile ale persoanei vizate.
- **Datele privind persoanele vizate vulnerabile** – prelucrarea acestui tip de date este un criteriu din cauza dezechilibrului de putere crescut între persoanele vizate și operatorul de date, ceea ce înseamnă că persoanele ar putea să nu fie în stare să-și dea cu ușurință consimțământul sau să se opună prelucrării datelor ori să își exercite drepturile. Persoanele vizate vulnerabile pot include copiii (deoarece aceștia pot fi considerați incapabili să se opună sau să consimtă ori să se opună în mod deliberat la prelucrarea datelor lor), angajați, segmente mai vulnerabile ale populației, care necesită protecție specială (ex.-persoane bolnave, solicitanți de azil, vârstnici, pacienți) și, în

orice caz, poate fi identificat un dezechilibru în relația dintre poziția persoanei vizate și operator.

- **Utilizarea inovatoare sau implementarea unor noi soluții tehnologice sau organizaționale**, cum ar fi, spre exemplu, combinarea utilizării impresiunilor digitale cu recunoașterea facială pentru îmbunătățirea controlului accesului fizic. RGPD clarifică faptul că utilizarea unor noi tehnologii, definite în conformitate cu nivelul atins al cunoștințelor tehnologice poate determina declanșarea unei evaluări a impactului. Acest lucru se datorează faptului că utilizarea unor astfel de tehnologii poate implica noi forme de colectare și utilizare a datelor, eventual cu un grad ridicat de risc pentru drepturile și libertățile persoanelor fizice. Într-adevăr, consecințele personale și sociale ale extensiei unei noi tehnologii pot fi necunoscute. O evaluare a impactului va ajuta operatorul să înțeleagă și să abordeze astfel de riscuri (ex. – anumite aplicații „Internet of Things" ar putea avea un impact semnificativ asupra vieții cotidiene private a persoanelor fizice și, ca atare, necesită o evaluare a impactului).
- **Atunci când prelucrarea în sine împiedică persoanele fizice să-și exercite un drept sau să utilizeze un serviciu sau un contract** (operațiuni de prelucrare care vizează permiterea, modificarea sau refuzarea accesului persoanelor fizice la un serviciu sau la încheierea unui contract). Putem fi în prezența unei astfel de situații atunci când, spre exemplu, o bancă procedează la verificarea clienților prin compararea cu o bază de date referitoare la credit pentru a decide acordarea unui împrumut.

Evaluarea impactului trebuie realizată anterior prelucrării, fapt ce evidențiază concordanța cu asigurarea protecției datelor începând cu momentul conceperii (privacy by design) și în mod implicit (privacy by default). De aceea, evaluarea impactului ar trebui văzută ca un instrument menit a ajuta la luarea deciziilor cu privire la prelucrare.

- **Formatul documentului în EXCEL se regăsește în ANEXA 20**

9.4 Gestionarea drepturilor persoanei vizate

Pornind de la drepturile persoanei vizate, enunțate anterior, în cele ce urmează, vom încerca să venim în sprijinul specialiștilor din cadrul MIPE, cu **recomandarea unor măsuri** de care trebuie să se țină cont atunci când, sunt elaborate Ghidurile Solicitanților pe diverse Programe Operaționale în vederea conformității cu prevederile RGPD.

- Dreptul la informare.

Pentru **punerea în practică** a acestui drept al persoanei vizate (obligație a Operatorului sau Persoanei Împuternicite de operator) ar trebui **prevăzut** în

capitolul referitor la „REGULI PENTRU ACORDAREA FINANȚĂRII" – subcapitolul Eligibilitatea Proiectului, printre condițiile pe care trebuie să le îndeplinească Proiectul și **următoarele condiții**:

- ✓ La elaborarea proiectelor să se țină cont de prevederile legislației interne și internaționale pe linie de protecție a prelucrării datelor cu caracter personal;
- ✓ Activitățile din proiecte propuse spre finanțare să fie analizate din punct de vedere al conformității cu RGPD
- ✓ Să fie implementate măsuri tehnice și organizatorice adecvate pentru protecția prelucrării datelor cu caracter personal ale grupului țintă căruia se adresează Proiectul
- ✓ Să fie efectuate evaluări ale studiului de impact în cazul constatării existenței unor riscuri în prelucrarea datelor cu caracter personal
- Drepturile persoanei vizate

Toate drepturile persoanei vizate prevăzute de RGPD trebuie respectate atât pe timpul pregătirii documentelor necesare pentru depunerea Cererii de Finanțare, cât și ulterior pe perioada derulării proiectelor aprobate.

În sprijinul activităților de gestionare, coordonare și control al specialiștilor din cadrul MIPE supunem atenției câteva documente strict necesare care trebuie elaborate de solicitanții de proiecte din fonduri FESI:

- Notă de informare a persoanei vizate cu privire la scopurile prelucrării datelor cu caracter personal în cadrul proiectului (atât pentru persoanele angajate și remunerate pentru implementarea proiectului, cât și pentru persoanele care fac parte din grupul țintă) – model orientativ Anexa 5
- Consimțământ al persoanei vizate dacă prelucrarea datelor se realizează pe baza acestui temei legal – model orientativ Anexa 6
- Documente de exercitare a drepturilor persoanelor vizate – model orientativ pentru Procedura de acces la date – Anexa 7
- Registrul de evidență a consimțămintelor – Anexa 8
- Registrul privind evidența solicitărilor persoanei vizate – Anexa 9

9.5 Elaborare și implementare proceduri

Cel mai important document care să contribuie la implementarea conformității RGPD, este Politica de prelucrare a datelor cu caracter personal, pe care trebuie să o elaboreze fiecare Operator.

Scopul Politicii îl reprezintă conformitatea cu dispozițiile 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) și a legislației naționale.

Politica se constituie ca instrument prin care organizația **se asigură că personalul** propriu, colaboratorii și partenerii **care prelucrează date** cu caracter personal pentru sau **în numele organizației** sunt conștienți de îndatoririle ce le revin și **se conformează procedurilor întocmite** și obligațiilor ce decurg din legislația privind protecția datelor cu caracter personal.

Scopul procedurilor îl constituie:

- stabilirea unui set unitar de reguli, măsuri tehnice și organizatorice adecvate pentru reglementarea aplicării unitare a măsurilor necesare pentru asigurarea protecției datelor cu caracter personal în cadrul îndeplinirii atribuțiilor de serviciu;
- stabilirea regulilor care trebuie urmate pentru soluționarea cererilor formulate de persoana vizată cu privire la datele cu caracter personal stocate și prelucrate de către organizație, sau în numele acesteia, stabilirea responsabilităților privind întocmirea, avizarea, aprobarea și transmiterea documentelor aferente acestei activități.

Prin politica de protecție a prelucrării datelor cu caracter personal pot fi prevăzute toate acele proceduri necesare a fi elaborate și prin care se stabilesc reguli și responsabilități pe linia protecției prelucrării datelor cu caracter personal care, vor fi considerate ca făcând parte (anexe) din politică.

Pentru a veni în sprijinul specialiștilor care au atribuții de gestionare, coordonare și control a proiectelor în contextul FESI prezentăm un model orientativ al acestui document – Anexa 10.

Acest model poate fi adaptat la cerințele proiectelor care sunt stabilite prin Ghidul solicitantului.

În vederea asigurării conformității cu prevederile RGPD, Operatorii care utilizează site-uri de prezentare sau de lucru trebuie să afișeze un capitol separat pentru politica de cookies-uri, sens în care trebuie să efectueze împreună cu specialiștii IT o analiză a vulnerabilităților site-ului și a cookies-urilor pe care acesta le utilizează.

Acest lucru este necesar pentru o elaborare a Politicii privind utilizarea cookies-urilor cât mai corectă care, să conțină în principal următoarele informații:

- ✓ date privind identitatea operatorului
- ✓ definiția cookie și la ce este utilizat
- ✓ de ce sunt utilizate cookies-urile

- ✓ ce categorii de cookie utilizează site-ul propriu
- ✓ cum pot fi oprite cookies-urile
- ✓ informații privind eventualele probleme în vizitarea site-ului dacă sunt oprite unele cookies-uri

De asemenea pe site va trebui să existe afișată Informarea (**Politica de confidențialitate**) prin care se comunică persoanelor vizate informațiile privind transparența prelucrării datelor cu caracter personal.

Acest document ar trebui să conțină în principal prevederile art. 13 din RGPD, respectiv:

- ✓ identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia;
- ✓ datele de contact ale responsabilului cu protecția datelor, după caz;
- ✓ scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;
- ✓ interesele legitime urmărite de operator sau de o parte terță, în cazul în care prelucrarea se efectuează într-un asemenea scop;
- ✓ destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- ✓ dacă este cazul, intenția operatorului de a transfera date cu caracter personal către o țară terță sau o organizație internațională și existența sau absența unei decizii a Comisiei Europene privind caracterul adecvat sau, în cazul transferurilor efectuate în baza unor garanții adecvate, a regulilor corporatiste obligatorii ori a unor derogări pentru situații specifice, o trimitere la garanțiile adecvate sau corespunzătoare și la mijloacele de a obține o copie a acestora, în cazul în care acestea au fost puse la dispoziție.
- ✓ perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
- ✓ existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora ori restricționarea prelucrării sau a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;
- ✓ atunci când prelucrarea datelor cu caracter personal, inclusiv a celor din categoriile speciale, are la bază consimțământul explicit al persoanei vizate, existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;
- ✓ dreptul de a depune o plângere în fața unei autorități de supraveghere;
- ✓ dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă persoana vizată este obligată să furnizeze aceste date cu

caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații;

- ✓ existența unui proces decizional automatizat incluzând crearea de profiluri și referitoare chiar și la prelucrări de categorii speciale de date cu caracter personal, precum și informații pertinente privind logica utilizată, importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată;
- ✓ informații privind scopul secundar al prelucrării și orice informații suplimentare relevante, în ipoteza în care operatorul intenționează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel inițial pentru care acestea au fost colectate.

9.6 Gestionarea drepturilor și alocarea responsabilităților angajaților

Acest capitol va aduce la cunoștința specialiștilor din cadrul MIPE cum trebuie controlate activitățile din cadrul proiectelor care asigură conformitatea cu RGPD

9.6.1. Gestionarea drepturilor angajaților în proiecte

- Identificarea modului de colectare pentru datele potențialilor angajați sau angajaților existenți în cadrul organizației, pentru derularea proiectului
  - ✓ Existența consimțămintelor potențialilor angajați pentru perioada dintre data depunerii Cererii de Finanțare și data încheierii contractelor de muncă după aprobarea acesteia;
  - ✓ Existența consimțămintelor angajaților existenți pentru prelucrarea datelor în condiții de beneficii suplimentare precum și utilizarea datelor în mod suplimentar (eventuale fotografii pe perioada de derulare a evenimentelor proiectului);
- Existența în cadrul Regulamentului Intern al proiectului a unor prevederi de prelucrare a datelor cu caracter personal care trebuie aduse la cunoștința tuturor participanților la proiect, respectiv:
  - ✓ Drepturi și obligații angajator privind prelucrarea datelor cu caracter personal:
    - Cum colectează datele
    - Ce date colectează
    - Cum utilizează datele
  - ✓ Drepturi și obligații angajat:
    - Respectarea confidențialității
    - Respectarea procedurilor de securitate și a politicilor
    - Drepturile instituite de RGPD

- Existența unei Proceduri pentru utilizarea unor mijloace tehnice puse la dispoziție în cadrul proiectului – model orientativ Anexa 11

- Existența unor reguli generale de securizare a datelor:

Lista enunțată nu este exhaustivă urmând a fi determinată de fiecare beneficiar de proiect în parte

- ✓ Utilizarea oricăror informații sau resurse informaționale care aparțin organizației pe timpul derulării proiectului în scopuri ilegale sau care nu servesc organizației este strict interzisă și poate duce la aplicarea de măsuri disciplinare;
- ✓ Înainte de orice transfer de informații ce conțin date cu caracter personal către un partener extern, emitentul (transmițătorul) va verifica dacă există un Acord de Confidențialitate sau o Clauză de Confidențialitate încheiată cu destinatarul și dacă datele ce urmează să fie transmise corespund naturii relației și comunicării cu destinatarul, în limitele dictate de procesele de eligibilitate și relații contractuale cu acesta;
- ✓ CUM SE VA COMUNICA ÎN CADRUL ACTIVITĂȚILOR PROIECTULUI - Pentru respectarea cadrului GDPR care reglementează transferul de date cu caracter personal, utilizatorul este obligat ca informația să fie adăugată într-o arhivă PAROLATĂ și apoi trimisă prin email către partenerii externi. Parola pentru deschiderea arhivei va fi comunicată destinatarului EXCLUSIV prin serviciul SMS.
- ✓ Orice dispozitiv de calcul cu caracter portabil (computer, memorie externă, dispozitive optice sau magnetice, telefon, etc.) care va accesa, gestiona sau transporta în mod direct informații cu caracter confidențial și/sau informații care conțin date cu caracter personal, trebuie să aplice criptarea datelor.
- ✓ Să fie interzis transferul de informații proprietatea organizației prin alte servicii de comunicații (ex. WhatsApp, Facebook, etc), precum și utilizarea email-urilor personale.
- ✓ Să fie strict interzisă comunicarea în afara organizației sau în afara grupului de confidențialitate asociat, a oricăror date sau documente ce au caracter intern, confidențial sau strict confidențial, pe orice formă (electronică, ca și copie pe dispozitive de stocare, email, postare pe web, copiere prin rețele date, fotografie sau fotocopie electronică, etc., scrisă/tipărită/fotocopie/fax sau verbală, comunicată direct, telefonic sau prin înregistrări audio), către orice alt terț în afară de cei autorizați din punct de vedere contractual prin clauze de confidențialitate în vigoare și în orice alt scop în afară de cel autorizat în cadrul proceselor de afacere;
- ✓ Să fie strict interzisă înregistrarea și filmarea prin resurse proprii și/sau fără autorizarea conducerii executive a discuțiilor de orice tip legate de procesul de prestări servici către grupul țintă;

- ✓ Nici un software nu trebuie să fie copiat, instalat sau distribuit în sistemele informatice ale proiectului fără o aprobare explicită a specialiștilor IT.
  De asemenea, este interzisă ocolirea mecanismelor preventive de securitate impuse de specialiștii IT pentru a preîntâmpina copierea, instalarea sau distribuirea software-ului sau a datelor deținute de organizație.
- ✓ Toate echipamentele portabile de calcul ale instituției trebuie să prezinte criptografie aplicată cu protecție cu parolă la accesul setărilor din BIOS, precum și la pornirea sistemului, înainte ca acesta să încarce sistemul de operare. Dacă sistemul portabil nu prezintă vreuna din aceste măsuri de protecție, utilizatorul are obligația de a contacta de urgență specialistul IT pentru a se informa de existența acesteia sau pentru programarea unei întrevederi ce va duce la corectarea acestei vulnerabilități;
- ✓ Trebuie să existe obligativitatea raportării către specialistul IT al oricărui furt sau pierdere a unui echipament IT mobil (telefon mobil, mijloc de stocare informații ce conține informații de serviciu, computer, token, card acces, etc.) pentru a se lua măsurile necesare de restricționare a accesului dispozitivelor pierdute la sistemele organizației;
- ✓ Trebuie să existe obligația ca pentru orice email ce prezintă caracter suspect, angajații în proiect, să ceară un punct de vedere colegilor din Departamentul IT înainte de a acționa în orice fel;
- ✓ Existența prevederilor că utilizatorii nu trebuie să utilizeze programe non-standard, cu licență limitată sau gratuită fără aprobarea specialistului IT al organizației, cu excepția celor aflate pe lista organizației;
- ✓ Să se interzică scoaterea neautorizată în afara sediului instituției a computerelor sau altor instrumente IT (în special cele care stochează date), fără acordul superiorului direct. La primirea solicitării privind părăsirea instituției cu echipamente IT, superiorul ierarhic are obligația să solicite un punct de vedere din partea specialistului IT privind măsurile de securitate de care dispozitivul IT beneficiază. Se vor avea în vedere cel puțin următoarele aspecte:
  - Mediul de stocare este criptat integral – acest aspect va oferi o garanție că în cazul unui furt sau pierdere, datele stocate nu vor putea fi accesate;
  - Datele din computer sunt salvate pe un suport extern al instituției – această condiție este strict necesară pentru a avea garanția recuperării integrale a datelor;
  - Utilizatorul a primit un set de instrucțiuni privind conectarea în siguranță la rețelele LAN sau Wireless externe.

Aceste condiții minime trebuie îndeplinite integral, dacă una sau mai multe condiții nu sunt îndeplinite, superiorul direct NU va trebui să aprobe solicitarea.

- ✓ Să existe obligativitatea ca în cazul în care un angajat află de o încălcare a dispozițiilor cuprinse în procedurile ce reglementează sfera securității informaționale, acesta să raporteze imediat superiorului ierarhic și responsabilului desemnat cu securitatea informațională;

9.6.2. Alocarea responsabilităților angajaților

- Implementarea de modificări ale Regulamentului intern, a politicilor și procedurilor existente pentru a include prevederi specifice în materia protecției datelor.

În cele ce urmează venim în sprijinul specialiștilor din MIPE cu unele documente orientative pentru a se inspira atunci când implementează conformitatea cu RGPD sau verifică modul de implementare în cazul proiectelor depuse pentru acordare finanțare.

Pe linia Regulamentului Intern un operator ar trebui să prevadă, așa cum reliefam anterior, toate situațiile în care colectează, utilizează și transmite datele cu caracter personal aparținând angajaților. În acest sens prezentăm un model de anexă la Regulamentul Intern de care fiecare angajat ia la cunoștință pe bază de semnătură la momentul semnării contractului de muncă – Anexa 11

- Elaborarea prevederilor și completări la fișa postului fiecărui angajat, în funcție de responsabilități

Pentru îndeplinirea acestui deziderat propunem un model orientativ de Completare a Fișei Postului – Anexa 12

Pe baza acestui model, pot fi incluse atribuții, sarcini și responsabilități pentru specialiști în Fișele Posturilor, conform posturilor pe care le ocupă în cadrul MIPE sau a nominalizărilor pe funcții în diverse proiecte.

- Elaborarea și implementarea procedurilor de raportare către DPO

Pentru punerea în aplicare a responsabilităților pe linia modului de lucru cu DPO aveți în anexa 3 un model orientativ al Procedurii de lucru cu DPO de unde se pot desprinde activitățile care trebuie respectate atunci când este necesar să fie implicat DPO.

- Elaborarea și implementarea procedurilor de raportare a incidentelor de securitate care conduc la încălcarea securității datelor cu caracter personal

Atunci când avem un incident de securitate se analizează natura acestuia și în funcție de rezultat se trece la o analiză mai profundă.

În situația în care incidentul este de natură informatică fără a afecta date cu caracter personal analiza se efectuează de către specialiștii IT conform procedurilor proprii.

În situația în care incidentul afectează date cu caracter personal este recomandat a se pune în aplicare prevederile Procedurii de răspuns în caz de încălcare a datelor cu caracter personal, în care un rol important îl joacă DPO.

Pentru exemplificarea modului de lucru în echipă în cazul unei încălcări a securității datelor cu caracter personal vă remitem un model orientativ al activităților prevăzute într-o procedură – Anexa 13

9.7 Creșterea gradului de conștientizare cu privire la confidențialitate și securitate

9.7.1 Organizarea sesiunilor de instruire

Periodic se recomandă organizarea de sesiuni de instruire în domeniul RGPD. Sesiunile de intruire trebuie adaptate la prelucrările efectuate de operatorul respectiv și în cazul proiectelor finanțate din fonduri FESI chiar adaptate prelucrărilor efectuate în cadrul proiectului. Se recomandă instruirea o data la 6 luni în cazul în care prelucrările privesc categorii speciale de date cu caracter personal.

9.8 Gestionarea arhivelor fizice

9.8.1 Elaborarea nomenclatorului arhivistic

- Emiterea deciziei interne pentru nominalizarea persoanelor care vor fi responsabile de inventarierea documentelor fiecărui departament sau nominalizarea unei singure persoane care să realizeze această inventariere.

Conform prevederilor legale incidente Legea 16 din 1996 privind arhivele naționale, cu modificările și completările ulterioare, fiecare entitate publică sau privată, trebuie să-și organizeze activitatea de arhivă în calitatea lor de creatori și deținători de documente.

În acest sens conducerea organizației stabilește împreună cu factorii de răspundere un Nomenclator Arhivistic în baza căruia stabilesc perioadele de păstrare a documentelor create, perioade care au la bază în primul rând legislația incidentă prin care aceste documente au fost impuse a fi create.

În cazul în care nu avem o legislație care să prevadă anumite termene de păstrare va trebui să se ia în calcul scopul creării documentelor și perioada după care expiră scopul pentru care au fost create.

Nomenclatorul astfel elaborat se trimite, conform prevederilor legale, la structura arhivelor naționale teritorială cu competență asupra sediului entității, în vederea aprobării.

- Inventarierea documentelor primite/elaborate, conform deciziei emise.

După fiecare an calendaristic la nivelul fiecărei entități se declanșează activitatea de arhivare a documentelor ce presupune o serie de activități printre care și inventarierea acestora. Această activitate este foarte laborioasă fapt pentru care vă propunem un model orientativ de procedură – Anexa 14

9.9 Calificarea contractelor

În cazul în care doi sau mai mulți operatori stabilesc în comun scopul și mijloacele de prelucrare, aceștia sunt **operatori asociați**. Ei **stabilesc** în mod transparent **responsabilitățile** fiecăruia în ceea ce privește îndeplinirea obligațiilor ce le revin potrivit RGPD, îndeosebi referitor la exercitarea drepturilor persoanelor vizate și la îndatoririle fiecăruia de furnizare a informațiilor de interes pentru persoana vizată, **prin intermediul unui acord** între ei, cu excepția cazului și în măsura în care responsabilitățile operatorilor sunt stabilite în dreptul UE sau în dreptul intern care se aplică acestora. **Acordul poate desemna un punct de contact pentru persoanele vizate** și reflectă in mod adecvat rolurile și raporturile respective ale operatorilor asociați față de persoanele vizate. Esența unui asemenea acord este făcută cunoscută persoanei vizate.

În cazul în care prelucrarea urmează să fie realizată în numele unui operator, acesta recurge doar la **persoane împuternicite** care oferă garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte cerințele prevăzute în RGPD și să asigure protecția drepturilor persoanei vizate.

Prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un contract sau alt act juridic în temeiul dreptului UE sau al dreptului intern, care are caracter obligatoriu pentru persoana împuternicită în raport cu operatorul și care stabilește obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate precum și obligațiile și drepturile operatorului. Contractul sau actul juridic prevede în special că persoana împuternicită de operator:

- prelucrează datele cu caracter personal numai pe baza unor instrucțiuni documentate din partea operatorului, inclusiv în ceea ce privește transferurile de date cu caracter personal către o țară terță sau o organizație internațională, cu excepția cazului în care această obligație îi revine persoanei împuternicite în temeiul dreptului UE sau al dreptului intern care i se aplică; într-o astfel de situație, va notifica această obligație juridică operatorului înainte de prelucrare, cu excepția cazului în care dreptul

respectiv interzice o astfel de notificare din motive importante legate de interesul public;

- se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidențialitatea sau au o obligație statutară adecvată de confidențialitate;
- adoptă toate măsurile necesare pentru asigurarea securității prelucrării datelor cu caracter personal;
- respectă toate condițiile prevăzute de RGPD privind recrutarea unei alte persoane împuternicite de operator;
- ținând seama de natura prelucrării, oferă asistență operatorului prin măsuri tehnice și 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 tuturor drepturilor prevăzute în Capitolul III din RGPD („Drepturile persoanei vizate");
- ajută operatorul să asigure respectarea obligațiilor privitoare la securitatea prelucrării datelor cu caracter personal, ținând seama de caracterul prelucrării și informațiile aflate la dispoziția persoanei împuternicite de operator;
- la alegerea operatorului, șterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare și elimină copiile existente, cu excepția cazului în care dreptul UE sau dreptul intern impune stocarea datelor cu caracter personal;
- pune la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea tuturor obligațiilor prezentate mai sus, permite desfășurarea auditurilor, inclusiv a inspecțiilor, efectuate de operator sau de alt auditor mandatat și contribuie la derularea acestora în cele mai bune condiții. Persoana împuternicită de operator informează imediat operatorul în cazul în care, în opinia sa, o instrucțiune încalcă RGPD sau alte dispoziții din dreptul intern sau din dreptul UE cu privire la protecția datelor cu caracter personal.

Aderarea persoanei împuternicite de operator la un cod de conduită aprobat sau la un mecanism de certificare aprobat poate fi utilizată ca element prin care se demonstrează existența garanțiilor suficiente în sensul conformității cu prevederile RGPD. În același timp, fără a aduce atingere în vreun fel unui contract individual încheiat între operator și persoana împuternicită de operator, contractul sau celălalt act juridic principal se poate fundamenta, integral sau parțial, pe clauze contractuale standard adoptate de autoritatea de supraveghere competentă, inclusiv atunci când fac parte dintr-o certificare acordată operatorului sau persoanei împuternicite de operator.

Persoana împuternicită de operator și orice persoană care acționează 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 UE sau dreptul intern le obligă să facă acest lucru.

1.1. Elaborare documente

- Draft acorduri specifice (împuterniciți și operatori asociați) și clauze contractuale minime

Pentru a înțelege mai bine cerințele RGPD în cazul prelucrărilor de date cu caracter personal în situațiile prezentate anterior, remitem un model orientativ de Acord între doi operatori asociați – Anexa 15

De asemenea remitem un model orientativ de Acord încheiat între un Operator și o Persoană Împuternicită de Operator – Anexa 16

- Draft Note de informare reprezentanți și persoane de contact, formulare de consimțământ

Prin aceste documente sunt informați reprezentanții partenerilor de contract și persoanelor de contact ai partenerilor cu privire la prelucrarea datelor cu caracter personal.

9.10 Identificarea contractelor

În cadrul acestei activități se analizează contractele semnate existente sau care urmează a fi încheiate pentru a se stabili calitatea celor doi parteneri.

În funcție de rezultatul analizei se vor elabora Acordurile de prelucrare a datelor cu caracter personal care, ulterior vor fi negociate în vederea semnării.

9.11 Securitate informațională

La nivelul operatorului se recomandă implementarea unei politici privind securitatea datelor cu caracter personal. Politica se recomandă a conține măsurile tehnice implementare la nivelul tuturor sistemelor care prelucrează date cu caracter personal.

9.12 Gestionarea persoanelor împuternicite de operator

- Elaborarea chestionarului de evaluare a persoanelor împuternicite

Acest document ne oferă posibilitatea ca, prin întrebările puse partenerului de contract să analizăm modul de conformare al acestuia cu prevederile RGPD. Ceea ce declară partenerul de contract pe propria răspundere se ia în calcul la semnarea contractului și poate fi verificat ulterior prin acțiuni de audit.

Un model orientativ este remis în Anexa 17

10. SECURITATE DATELOR CU CARACTER PERSONAL

10.1 Despre securitatea datelor cu caracter personal

Un principiu cheie al GDPR este că prelucrarea datelor cu caracter personal trebuie să aibă loc în siguranță prin implementarea unor măsuri tehnice și organizatorice adecvate.

Acesta reprezintă principiul securității datelor cu caracter personal, iar acest principiu presupune aspecte precum analiza riscurilor, implementarea de politici și proceduri organizaționale precum și de măsuri fizice și tehnice de protecție a datelor cu caracter personal.

> Art. 5 alin. (1), litera f. din RGPD prevede ca datele cu caracter personal să fie:
> (f) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare ("integritate și confidențialitate").

Aceasta înseamnă că operatorul trebuie să implementeze măsuri de securitate adecvate pentru a preveni compromiterea accidentală sau deliberată a datelor personale pe care le deține. Trebuie să se țină cont și de faptul că securitatea informaţiilor cu toate că este uneori considerată drept o securitate cibernetică (protecția rețelelor şi a sistemelor de informații împotriva atacurilor), aceasta acoperă şi alte aspecte, cum ar fi măsurile de securitate fizică şi organizatorică.

> Art. 32 din RGPD, alin. (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;
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.

Art. 32 din RGPD, alin. (2), (3), (4)
(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) Aderarea la un cod de conduită aprobat, menționat la articolul 40, sau la un mecanism de certificare aprobat, menționat la articolul 42, poate fi utilizată ca element prin care să se demonstreze îndeplinirea cerințelor prevăzute la alineatul (1) din prezentul articol.
(4) 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.

Art. 32, prin aliniatele sale specifică printre altele, că securitatea datelor cu caracter personal trebuie să fie o preocupare și a persoanelor împuternicite ale operatorului, acesta acționând sub autoritatea operatorului.

RGPD nu stabilește un set de măsuri de securitate pe care operatorului trebuie să le aibă în vedere, ci lasă operatorului libertatea de a alege măsurile potrivite în funție de „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".

Acest lucru reflectă atât abordarea bazată pe risc a RGPD, cât şi faptul că nu există o soluţie *"de o mărime potrivită"* pentru securitatea informaţiilor.

Aceasta înseamnă că ceea ce este "potrivit" pentru un operator nu este neapărat potrivit pentru altul.

Deci, înainte de a decide ce măsuri sunt adecvate, trebuie evaluat riscul de confidențialitate.

Operatorul trebuie să revizuiască datele personale pe care le deține, modul în care le utilizează, clasificarea în cât de sensibile sau confidențiale sunt, precum și daunele și prejudiciile care ar putea fi cauzate în cazul în care datele ar fi compromise.

Operatorul poate ține cont și de alți factori, precum:

- Natura și amploarea prelucrării;
- Numărul de persoane care accesează datele cu caracter personal;
- Numărul de împuterniciți, localizarea împuterniciților, etc.

10.2 Prejudiciile unei securități slabe

O securitate slabă a informaţiilor pun în pericol şi poate provoca vătămări şi suferinţe reale persoanelor - vieţile pot fi chiar periclitate în anumite cazuri extreme.

Câteva exemple de prejudicii cauzate de pierderea sau abuzul de date cu caracter personal includ:

- furtul de identitate; tranzacţii false de cărţi de credit;
- targetarea persoanelor de către infractori, care ar putea deveni mai convingătoare prin datele personale compromise;
- martori expuşi riscului de vătămare corporală sau de intimidare;
- infractorii aflaţi în pericol de persoane care vor să se răzbune;
- expunerea adreselor personalului de serviciu, poliţiştilor şi ofiţerilor de penitenciare şi celor expuşi riscului de violenţă în familie; cererile false pentru credite şi fraudă ipotecară.

Cu toate că aceste consecințe nu se întâmplă întotdeauna, trebuie să recunoașteți că persoanele sunt în continuare îndreptățite să fie protejate împotriva unor vătămări mai puțin grave, de exemplu un pericol de imagine.

Securitatea informațiilor este importantă, nu numai pentru că ea însăși este o cerință legală, ci și pentru că poate sprijini buna guvernanță a datelor și vă poate ajuta să demonstrați conformitatea cu alte aspecte ale RGPD.

10.3 Exemple de Măsuri tehnice și de securitate adecvate

O lista de exemple de măsuri tehnice și de securitate se regăsește în cele ce urmează. **Atenție! Lista este cu caracter de exemplu. Măsurile exacte se stabilesc în urma analizei de risc efectuate de către fiecare operator.**

1. Configurarea accesului la resursele interne ale instituției cu ajutorul conturilor de tip VPN (Virtual Private Network), ce asigură accesul și transferul datelor în mod criptat și securizat.
2. Activarea unui serviciu de securizare a infrastructurii IT din instituție, prin oferirea de acces centralizat, cu posibilitatea de a crea politici de securizare a accesului prin: parole și acces pe resursele de tip documente ale instituției în funcție de drepturile alocate, care să ofere actualizări în mod centralizat pentru toate stațiile de lucru: Microsoft
3. Windows server cu rol de Active Directory, File Server, Print Server, Windows Update Server, etc.
4. Implementarea de politici de securitate pentru accesul la stațiile de lucru, prin acces pe bază de user și parolă. Crearea de conturi nominale pentru utilizatori și dezactivarea celor cu nume generic.
5. Aplicarea de politici de securizare a parolei: schimbare la timp predefinit - cel puțin 42 de zile, să aibă cel puțin 8 caractere, să respecte normele Microsoft de complexitate (litere MARI, litere mici, cifre și semne de punctuație). Stațiile de lucru configurate să se blocheze automat în momentele de inactivitate și la reluarea activității să ceară parola utilizatorului, pentru a preveni accesul neautorizat la stațiile de lucru.
6. Securizarea accesului la stațiile de lucru prin folosirea de drepturi adecvate ale utilizatorilor. Configurarea conturilor cu drepturi limitate de acces și eliminarea drepturilor de tip administrator de pe stațiile de lucru, pentru toți utilizatorii.
7. Implementare de politici de securizare a accesului la stațiile de lucru cu stick-uri de tip USB sau alte echipamente portabile de stocare a datelor. Acceptarea transferului de date doar către echipamentele portabile acceptate în instituție. Criptarea acestor echipamente portabile de transfer a datelor.
8. Integrarea echipamentului de tip Next Generation Firewall cu Active Directory și acordarea de acces în interiorul instituției (acces VPN) prin

intermediul userilor și a parolelor din domeniu - acces centralizat la resursele instituției.

9. Implementarea unei politici de criptare a stațiilor de lucru și a laptopurilor folosind soluții native Microsoft sau alte soluții.
10. Implementarea unei politici de eliminare a programelor nedorite de pe stațiile de lucru. Eliminarea programelor de acces de la distanță de pe stațiile de lucru.
11. Implementarea unei soluții antivirus comerciale cu suport și actualizări din partea producătorului și configurarea acesteia cu consola de management centralizat pentru TOATE stațiile de lucru din instituție. Configurarea soluției cu politici de securitate: actualizarea semnăturilor în fiecare oră, actualizarea programului odată la 6 ore, protejarea setărilor cu parolă astfel încât utilizatorii să nu poată opri protecția antivirus, crearea de task-uri de scanare automată a stațiilor la un timp predefinit.
12. Eliminarea programelor antivirus gratuite de pe computerele PS1 și înlocuirea lor cu soluții antivirus profesioniste cu suport comercial și cu consolă de management centralizat, ce permite monitorizarea în timp real a situației actualizărilor semnăturilor.
13. Eliminarea programelor de acces de la distanță de tip Team Viewer de pe stațiile de lucru. Pot fi extrase date din instituție!
14. Folosirea unei soluții specializate de tip Firewall pe stațiile de lucru, eventual activarea funcției de tip Firewall a soluției antivirus. Eliminarea tuturor excepțiilor din Windows Firewall și configurarea restrictivă a acestuia.
15. Configurarea corectă a serviciului de actualizări Windows, astfel încât stațiile de lucru să primească cu precădere actualizări de securitate ale sistemului de operare și configurarea serviciului să restarteze calculatoarele în timp rezonabil, astfel încât să nu impacteze activitatea utilizatorilor. Eventual implementarea unui serviciu specializat de actualizare a stațiilor de lucru cu sistem de operare Windows - Server Update Services. Realizarea unei proceduri de Patch Management.
16. Sincronizarea ceasurilor tuturor echipamentelor din infrastructura IT cu același server de tip NTP (Network Time Protocol) - Echipamente de rețea, servere, stații de lucru.
17. Implementarea unui server de fișiere (File Server) dedicat, cu o structură de directoare ce să reflecte cât mai bine departamentele și nevoile instituției. Implementarea de politici de securizare a accesului la fișiere folosind drepturi de acces conform utilizatorilor din instituție. Implementarea unei politici de lucru centralizat cu fișierele pe server și nu descentralziat pe stațiile de lucru. Mutarea tuturor documentelor de pe stațiile de lucru pe serverul de fișiere pentru a beneficia de măsuri de securitate superioare.
18. Dezactivarea tuturor folderelor partajate din rețea, de pe toate stațiile de lucru. Folosirea serverului de fișiere implementat.
19. Implementarea unei soluții de back-up al documentelor, folosind un echipament extern de stocare a datelor. Realizarea de politici de back-up automatizat și versionat a datelor pe echipamentul extern de stocare.

Implementarea unei soluții de back-up a datelor în afara instituției, realizarea unei proceduri de Business Continuity și Disaster Recovery.

20. Realizarea unor proceduri de criptare a back-up-ului în tranzit și în staționare. Implementarea unor proceduri de verificare periodică a integrității salvărilor de tip back-up.
21. 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 atacuri și descoperirea de vulnerabilități.
22. Realizarea de teste periodice de penetrare a site-urilor instituției pentru descoperirea posibilelor vulnerabilități existente și pentru a testa reziliența site-urilor la atacurile malițioase din Internet.
23. Implementarea unui echipament sau a unui serviciu de tip Web Application Firewall (WAF) care să asigure protecția site-urilor instituției împotriva atacurilor malițioase din Internet. Configurarea acestuia pentru a bloca atacurile cele mai comune: cross-site scripting, SQL injection și file inclusion.
24. Implementarea de politici de securizare a accesului la platforma de administrare a bazelor de date ale site-urilor instituției. Restricționarea accesului doar de la anumite adrese IP și realizarea comunicării pe canal criptat - HTTPS, opțional: implementarea de acces securizat prin VPN. Implementarea de politici de securizare a conturilor - conturi nominale și a parolei de acces - parola complexă și care se schimbă la o perioadă predefinită de timp de maximum 60 zile.
25. Implementarea unei proceduri de jurnalizare a accesului furnizorului extern de servicii IT pe serverele instituției, astfel încât să existe o trasabilitate a acțiunilor întreprinse.
26. Implementarea unui serviciu de monitorizare în timp real a incidentelor de securitate IT - SIEM (Security Information and Event Management), pentru a putea preveni și descoperi breșele de securitate ce trebuiesc anunțate către Autoritatea de Supraveghere. Monitorizarea tuturor sistemelor IT din cadrul instituției: echipamente de rețelistică, firewall, servere, echipamente de backup, stații de lucru etc - conformitate cu art. 33 din Regulament.
27. Realizarea și implementarea unei proceduri de tratare a incidentelor de securitate.
28. Implementarea unor proceduri de criptare a mailurilor și de asemenea de criptare a documentelor ce sunt trimise pe mail în afara instituției.
29. Realizarea unei proceduri de securizare cu parolă/ cod PIN și criptare a telefoanelor instituției ce sunt utilizate de angajați.
30. Verificarea și reconfigurarea clienților mail (unde este cazul), de pe telefoanele ce părăsesc instituția, astfel încât să se folosească protocoale SSL/TLS de criptare a traficului cu serverul de mail.
31. Verificarea și reconfigurarea clienților mail (unde este cazul), de pe laptopurile ce părăsesc instituția, astfel încât să se folosească DOAR protocolul IMAP securizat cu certificate SSL/TLS de criptare a traficului cu serverul de mail.

32. Implementarea unei politici de securizare a parolei conturilor de mail - folosirea de parole complexe. De asemenea implementarea unui proces de schimbare periodică a acestor parole.
33. Realizare politică și procedură de lucru pe serverul de fișiere intern, cu acces securizat prin user intern și parolă, cu acces din exteriorul instituției prin canal criptat de comunicație (cont VPN).
34. Asigurarea protecției fizice adecvate pentru echipamentele din camera unde este găzduit serverul intern. Realizarea unui jurnal cu evidențe de acces în această cameră, pentru a avea trasabilitatea accesului fizic la serverele instituției.
35. Asigurarea unei temperaturi optime de lucru pentru echipamentele din camera serverelor.
36. Verificarea echipamentelor de protecție împotriva vârfurilor de tensiune - UPS, din camera serverelor. Realizarea de teste de performanță și înlocuirea lor acolo unde este cazul. Conectarea tuturor echipamentelor la UPS-uri.
37. Asigurarea protecției fizice adecvate pentru echipamentele de tip DVR/NVR. Securizarea lor în rack-uri specializate, închise cu cheie.
38. Verificarea echipamentelor de tip UPS ce oferă protecție împotriva vârfurilor de tensiune pentru echipamentele de tip DVR/NVR din toată infrastructura.
39. RECOMANDARE OPȚIONALĂ: implementarea unui provider secundar de Internet, are să asigure funcționalitatea continuă a serviciului de acces la Internet

10.4 Incidența măsurilor de securitate asupra aplicației MYSMIS

Sistemul MySMIS 2014 reprezintă un instrument/sistem utilizat în gestiunea proiectelor finanțate din Fonduri Europene Structurale și de Investiții/(FESI).

Atunci când se realizează cartografierea datelor cu caracter personal utilizate în procesele instituției, sau a proiectelor, principiile RGPD trebuie extinse și aplicate atât la nivelul prelucrărilor efectuate în format fizic cât și la nivelul prelucrărilor efectuate în sisteme/soluții informatice. Exemplu: ștergerea datelor nu se efectuează doar la nivelul documentelor prin distrugerea acestora, ci și la nivelul sistemelor/soluțiilor utilizate în prelucrarea datelor.

Având în vedere natura și scopul sistemului MySMIS și anume colector de date cu caracter personal, se recomandă ca acesta să respecte standarde ridicate de protecție a datelor cu caracter personal.

Trebuie să se țină cont că o analiză detaliată este necesară în vederea stabilirii măsurilor exacte.

- Managementul accesului
  - ✓ Implementarea de politici de securizare a accesului la platformă prin definirea unei matrici de acces la sistem prin separarea sarcinilor și responsabilităților;

- ✓ Matricea implementată să țină cont și de drepturile de descărcare a documentelor stocate în MySMIS;
- ✓ Implementarea unor politici/proceduri de acces la bazele de date, serverele de aplicații astfel încât doar personalul autorizat să aibă acces la aceste resurse;
- ✓ Implementarea de proceduri de retragere a accesului utilizatorilor de îndată ce aceștia nu mai sunt autorizați să utilizeze resursele;
- ✓ Efectuarea unei analize anuale privind drepturile de acces.

➢ Autentificarea utilizatorilor
- ✓ Definirea pentru fiecare utilizator unui identificator unic;
- ✓ Aplicarea de politici de securizare a parolei: schimbare la timp predefinit - cel puțin 42 de zile, să aibă cel puțin 8 caractere, să respecte normele de complexitate (litere MARI, litere mici, cifre și semne de punctuație).

➢ Monitorizarea accesului și 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;
- ✓ 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 atacuri și descoperirea de vulnerabilități;
- ✓ Realizarea de teste periodice de penetrare pentru descoperirea posibilelor vulnerabilități existente și pentru a testa reziliența la atacurile malițioase din Internet;
- ✓ Realizarea și implementarea unei proceduri de tratare a incidentelor de securitate.

➢ Protejarea stațiilor de lucru ale utilizatorilor Sistemului MySMIS, în special cei care au drepturi de descărcare documente din sistem.
- ✓ Implementarea de politici de securitate pentru accesul la stațiile de lucru, prin acces pe bază de user și parolă. Crearea de conturi nominale pentru utilizatori și dezactivarea celor cu nume generic;
- ✓ Aplicarea de politici de securizare a parolei: schimbare la timp predefinit - cel puțin 60 de zile, să aibă cel puțin 8 caractere, să respecte normele de complexitate (litere MARI, litere mici, cifre și semne de punctuație).
- ✓ Stațiile de lucru configurate să se blocheze automat în momentele de inactivitate și la reluarea activității să ceară parola utilizatorului, pentru a preveni accesului neautorizat la stațiile de lucru;
- ✓ USB sau alte echipamente portabile de stocare a datelor. Acceptarea transferului de date doar către echipamentele portabile acceptate în instituție. Criptarea acestor echipamente portabile de transfer a datelor;

- ✓ Implementarea unei soluții antivirus comerciale cu suport și actualizări din partea producătorului.
- ✓ Eliminarea programelor antivirus gratuite de pe computerele utilizatorilor și înlocuirea lor cu soluții antivirus profesioniste cu suport comercial și cu consolă 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. Pot fi extrase date din instituție!

➢ Protejarea rețelei interne
- ✓ Limitarea accesului la serviciile neesențiale (VoIP, peer to peer, etc.)
- ✓ 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 (cartelă inteligentă, parolă unică generată de fiecare dată etc.).
- ✓ Asigurarea că nicio interfață de administrare nu este direct accesibilă de pe Internet, iar întreținerea la distanță este realizată printr-o rețea VPN.

➢ Asigurarea continuității activității
- ✓ Efectuarea de copii de siguranță, periodic, protejarea acestora asigurând același nivel de securitate ca și cel pentru datele stocate pe serverele operaționale;
- ✓ Proceduri backup, implementare sisteme securitate backup: firewall;
- ✓ Testare periodică (anuală) a vulnerabilităților și punerea în aplicare a unui Plan de Continuitate;
- ✓ Cumpărarea de generatoare/baterii pentru serverele locale; contractarea și impunerea asigurării continuității furnizării energiei electrice la serverele de stocare. Utilizarea unei surse de alimentare continuă pentru a proteja echipamentul utilizat;
- ✓ RECOMANDARE OPȚIONALĂ: implementarea unui provider secundar de Internet, are să asigure funcționalitatea continua a serviciului de acces la Internet.

➢ Arhivarea securizată / stocarea electronică a documentelor
- ✓ 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 stocurile de documente care conțin date;
- ✓ Aplicarea de măsuri care să garanteze distrugerea arhivei electronice în întregimea sa, inclusiv back-ul arhivelor;

➢ Serverele
- ✓ Sincronizarea ceasurilor tuturor echipamentelor din infrastructura IT cu același server de tip NTP (Network Time Protocol) - Echipamente de rețea, servere, stații de lucru;
- ✓ Asigurarea protecției fizice adecvate pentru echipamentele din camera unde este găzduit serverul intern. Realizarea unui jurnal cu evidențe de acces în

această cameră, pentru a avea trasabilitatea accesului fizic la serverele pe care este gazduită soluția;
- ✓ Asigurarea unei temperaturi optime de lucru pentru echipamentele din camera serverelor;
- ✓ Verificarea echipamentelor de protecție împotriva vârfurilor de tensiune - UPS, din camera serverelor. Realizarea de teste de performanță și înlocuirea lor acolo unde este cazul. Conectarea tuturor echipamentelor la UPS-uri.
- ✓ Asigurarea protecției fizice adecvate pentru echipamentele de tip DVR/NVR. Securizarea lor în rack-uri specializate, închise cu cheie.
- ✓ Verificarea echipamentelor de tip UPS ce oferă protecție împotriva vârfurilor de tensiune pentru echipamentele de tip DVR/NVR din toată infrastructura.

11. DPIA – EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR

Evaluarea impactului asupra protecției datelor, cunoscută și sub acronimul DPIA, este o cerință obligatorie în cadrul RGPD conform Articolului 35. Acest articol oferă îndrumare referitor la momentul și modalitatea realizării acestuia, precizând:

> *„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."*

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

DPIA reprezintă un instrument important pentru responsabilizare deoarece ajută operatorii de date nu numai să respecte cerințele GDPR, ci și să demonstreze că au fost luate măsuri adecvate pentru a asigura conformitatea cu Regulamentul (Art. 24 GDPR).

Cu alte cuvinte, **DPIA reprezintă un proces pentru construirea și demonstrarea conformității.**

11.1 Când este necesară o DPIA?

În conformitate cu abordarea bazată pe risc, implementată de GDPR, realizarea unei DPIA nu este obligatorie pentru fiecare operațiune de prelucrare. DPIA este necesară numai atunci când prelucrarea este „susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice" (art. 35 (1)).

Pentru a asigura o interpretare consecventă a circumstanțelor în care o DPIA este obligatorie, în conformitate cu aliniatul 4, al art.35, *„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). Autoritatea de supraveghere comunică aceste liste comitetului menționat la articolul 68."*

11.2 De ce este necesară o DPIA?

RGPD cere operatorilor să implementeze măsuri adecvate pentru a asigura şi demonstra conformitatea cu GDPR, luand în considerare, printre altele, „riscurile de variație a probabilității și gravității asupra drepturilor și libertăților persoanelor fizice" (art. 24(1)).

Obligația operatorilor de a realiza DPIA în anumite situaţii ar trebui înțeleasă în contextul obligaţiei lor generale de a gestiona în mod corespunzător riscurile prezentate de prelucrarea datelor cu caracter personal.

11.3 Când este necesară o DPIA conform Decizie 174 / 2018 ANSDPC?

Conform Art. 1 alin. (1) al Deciziei 174/2018 a ANSDPC Evaluarea impactului asupra protecţiei 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 şi cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, şi care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;
b) prelucrarea pe scară largă a datelor cu caracter personal privind originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenenţa la sindicate, a datelor genetice, a datelor biometrice pentru identificarea unică a unei persoane fizice, a datelor privind sănătatea, viaţa sexuală sau orientarea sexuală ale unei persoane fizice sau a datelor cu caracter personal referitoare la condamnări penale şi infracţiuni;
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, pieţe, parcuri sau alte asemenea spaţii;
d) prelucrarea pe scară largă a datelor cu caracter personal ale persoanelor vulnerabile, în special ale minorilor şi ale angajaţilor, prin mijloace automate

de monitorizare şi/sau înregistrare sistematică a comportamentului, inclusiv în vederea desfăşurării activităţilor de reclamă, marketing şi publicitate;

e) prelucrarea pe scară largă a datelor cu caracter personal prin utilizarea inovatoare sau implementarea unor tehnologii noi, în special în cazul în care operaţiunile respective limitează capacitatea persoanelor vizate de a-şi exercita drepturile, cum ar fi utilizarea tehnicilor de recunoaştere facială în vederea facilitării accesului în diferite spaţii;
f) prelucrarea pe scară largă a datelor generate de dispozitive cu senzori care transmit date prin internet sau prin alte mijloace (aplicaţii "Internetul lucrurilor", cum ar fi smart TV, vehicule conectate, contoare inteligente, jucării inteligente, oraşe inteligente sau alte asemenea aplicaţii);
g) prelucrarea pe scară largă şi/sau sistematică a datelor de trafic şi/sau de localizare a persoanelor fizice (cum ar fi monitorizarea prin Wi-Fi, prelucrarea datelor de localizare geografică a pasagerilor în transportul public sau alte asemenea situaţii) atunci când prelucrarea nu este necesară pentru prestarea unui serviciu solicitat de persoana vizată.

11.4 Când nu este necesară o DPIA?

(2) Prin excepţie de la **alin. (1),** evaluarea impactului asupra protecţiei datelor nu este obligatorie atunci când:

a) prelucrarea efectuată în temeiul art. 6 alin. (1) lit. (c) sau (e) din Regulamentul general privind protecţia datelor are un temei juridic în dreptul Uniunii sau în dreptul intern şi deja s-a efectuat o evaluare a impactului asupra protecţiei datelor ca parte a unei evaluări generale a impactului în contextul adoptării actelor normative respective.

Atenţie!

Simplul fapt că condițiile care declanșează obligația de a realiza DPIA nu au fost indeplinite nu diminuează, însă, obligația generală a operatorilor de a implementa măsuri corespunzătoare pentru gestionarea adecvată a riscurilor asupra drepturilor și libertăților persoanelor vizate. În practică, acest lucru înseamnă că operatorii trebuie să evalueze în mod continuu riscurile create de activitățile lor de prelucrare pentru a identifica momentul în care un tip de prelucrare „ar putea duce la un risc ridicat pentru drepturile și libertățile persoanelor fizice".

11.5 Managementul riscurilor

11.5.1 Identificarea riscurilor

"Drepturile și libertățile" persoanei vizate se referă în principal la dreptul la viață privată, dar ar putea include și:

- libertate de exprimare
- libertatea de gândire

- libertate de mișcare
- interzicerea discriminării
- dreptul la libertate, conștiință și religie

De asemenea, ar putea fi oportun să se ia în considerare și alte efecte asupra persoanei vizate, în funcție de circumstanțele specifice și de natura prelucrării.

Procesul de identificare a riscurilor pentru drepturile și libertățile persoanelor fizice care rezultă din prelucrarea datelor cu caracter personal colectate, procesate și deținute va consta în mai mulți pași.

Identificarea riscurilor va fi efectuată printr-o combinație de discuții de grup și interviu cu părțile interesate. Astfel de părți interesate includ în mod normal (dacă este posibil):

- Manager(i) responsabil(i) pentru fiecare activitate
- Reprezentanți ai persoanelor care derulează în mod normal fiecare activitate
- Furnizorii de inputuri privind activitatea (inclusiv, dacă este cazul, persoana vizată)
- Destinatarii rezultatelor activității
- Terțe părți cu cunoștințe relevante
- Reprezentanții celor care furnizează resurse și servicii suport pentru activitate
- Orice altă parte considerată a oferi o contribuție utilă la procesul de identificare a riscurilor

Riscurile identificate vor fi înregistrate cu o descriere cât mai completă posibil care să permită evaluarea probabilității și a impactului riscului. Fiecare risc ar trebui să fie, de asemenea, alocat unui owner/titular.

11.5.2 Analiza riscurilor

Analiza riscului în cadrul acestui proces implică atribuirea unei valori numerice a) probabilității și b) impactului unui risc. Aceste valori sunt apoi combinate pentru a ajunge la un nivel de clasificare ridicat, mediu sau scăzut al riscului.

11.5.2.1 Evaluarea probabilității

Trebuie realizată o estimare a probabilităților de materializare a riscului. Aceasta trebuie realizată ținând cont de împrejurarea că riscul s-a materializat în trecut în cadrul organizației sau în cadrul unor organizații similare din aceeași ramură sau locație sau că există suficiente motive, oportunități sau capacități ca o amenințare să devină activă.

Probabilitatea de producere a fiecărui risc trebuie numerotată pe o scară numerică de la 1 (scăzut) la 5 (ridicat).

Instrucțiuni generale pentru definirea fiecărui grad de risc sunt menționate în tabelul de mai jos. Când se estimează probabilitățile de materializare a riscului, măsurile existente pentru contracararea riscului, ca și eficacitatea acestora, trebuie avute în vedere.

Gradul	Descrierea	Sumar
1	Improbabil	Niciodată nu s-a concretizat și nu există motive ca s-ar putea concretiza în viitor
2	Puțin Posibil	Există o posibilitate de a se concretiza, dar probabil nu se va concretiza
3	Posibil	Riscul are mai multe șanse de a se concretiza decât a nu se concretiza
4	Foarte posibil	Ar fi o surpriză ca riscul să nu se concretizeze, fie bazat pe experiențe similare din trecut, fie bazat pe circumstanțe curente
5	Aproape sigur	Ori se concretizează în mod frecvent, ori există motive întemeiate de a crede că este iminent

Argumentarea alocării gradului de probabilitate a riscului trebuie înregistrată pentru a facilita înțelegerea și a asigura repetabilitatea în evaluări viitoare și consecvența modului de evaluare.

11.5.2.2 Evaluarea impactului

Trebuie realizată o estimare a impactului pe care un risc anume îl poate avea asupra drepturilor si libertăților persoanei vizate. Această estimare trebuie sa ia in considerare măsurile existente care sunt de natură să diminueze impactul, atâta timp cât aceste măsuri sunt eficiente.

Trebuie acordată atenție impactului cel puțin în următoarele domenii:

- Financiar
- Sănătate si Siguranță
- Reputație
- Obligații legale, contractuale sau de compliance
- Alte impacturi potențiale

Impactul fiecărui risc trebuie numerotat pe o scară numerică de la 1 (scăzut) la 5 (foarte ridicat).

Instrucțiuni generale pentru definirea fiecărui grad sunt menționate în tabelul următor. Argumentarea alocării gradului de impact al riscului trebuie înregistrată pentru a facilita înțelegerea și a asigura repetabilitatea în evaluări viitoare.

Gradul	Descrierea	Impactul Financiar	Sănătate si Siguranță	Impactul asupra Reputației	Impactul Legal	Alte impacturi potențiale

1	Neglijabil	Definiți linii directoare	Definiți linii directoare	Definiți linii directoare	Definiți linii directoare	Definiți linii directoare
2	Ușoară	Definiți linii directoare	Definiți linii directoare	Definiți linii directoare	Definiți linii directoare	Definiți linii directoare
3	Moderată	Definiți linii directoare	Definiți linii directoare	Definiți linii directoare	Definiți linii directoare	Definiți linii directoare
4	Ridicată	Definiți linii directoare	Definiți linii directoare	Definiți linii directoare	Definiți linii directoare	Definiți linii directoare
5	Foarte Ridicată	Definiți linii directoare	Definiți linii directoare	Definiți linii directoare	Definiți linii directoare	Definiți linii directoare

11.5.2.3 Clasificarea riscurilor

Se va calcula un scor, bazat pe evaluarea gradului de probabilitate și de impact, combinând/înmulțind cele două valori, una aferent probabilității și una aferent impactului. Scorul rezultat este utilizat pentru a se decide clasificarea riscului având drept model matricea de mai jos.

Fiecărui risc îi va fi alocată o clasificare bazată pe scorul obținut, astfel:

- RIDICAT - 12 sau mai mult
- MEDIU - între 5 și 10 inclusiv
- SCĂZUT - de la 1 la 4 inclusiv

Probabilitatea riscului						
	5					
	4					
	3					
	2					
	1					
		1	2	3	4	5
	Impactul riscului					

Clasificarea fiecărui risc va fi înregistrată ca element introductiv în etapa de evaluare a riscului.

11.5.3 Evaluarea riscurilor

Scopul evaluării riscului este de a decide care riscuri sunt acceptabile și care riscuri trebuie gestionate/tratate.

Prioritizarea gestionării/tratării riscurilor se face în funcție de scorul obținut și clasificarea lor, iar din acest punct de vedere se recomandă ca riscurile cu un scor foarte mare să fie abordate înaintea celor cu un risc scăzut.

11.5.4 Definirea planului de tratare/gestionare a riscurilor

Atunci când sunt identificate riscuri de nivel dincolo de toleranță, se aplică mijloace de tratare/gestionare a lor.

Intenția generală a gestionării riscului este de a reduce clasificarea unui risc la un nivel acceptabil. Acest lucru poate fi imposibil în anumite cazuri în care, deși scorul este redus, riscul rămâne în aceeași zonă de clasificare - de exemplu se reduce scorul de la 8 la 6, dar riscul rămâne la nivelul mediu de clasificare. Operatorul poate decide să accepte aceste riscuri chiar dacă ele rămân la nivelul mediu de clasificare. Astfel de decizii trebuie înregistrate împreună cu explicația adecvată.

11.5.5 Opțiunile de tratare a riscurilor

Următoarele opțiuni pot fi utilizate pentru tratamentul riscurilor în legătură cu care s-a stabilit că sunt de neacceptat:

1. Modificarea riscului – se aplică măsuri adecvate pentru a micșora probabilitatea și/sau impactul riscului

2. Evitarea riscului prin luarea de măsuri pentru a nu se ajunge la realizarea acestuia

3. Împărțirea riscului cu o terță parte - de exemplu asigurător sau furnizor

Strategia va fi decisă pe baza cunoașterii clare a circumstanțelor riscului, ca de exemplu:

- Strategia de Afaceri
- Considerații legislative și de reglementare
- Probleme Tehnice
- Probleme comerciale și contractuale

Ofițerul pentru protecția datelor (DPO) se va asigura că toate părțile interesate sunt consultate, inclusiv titularul riscului.

11.5.6 Selecția măsurilor

Vor fi identificate măsurile adecvate - acțiuni care vor fi utilizate pentru a gestiona riscul – pentru a reduce probabilitatea și impactul fiecărui risc și pentru a-l aduce în limite acceptabile.

Pot fi folosite măsuri din Standardul ISO/IEC 27001 – Securitatea Informațiilor, precum și ISO/IEC 27002 – Codul de practică pentru controalele de securitate a informațiilor, ISO/IEC 27017 – Codul de practică pentru controalele de securitate a informațiilor bazat pe ISO/IEC 27002 pentru servicii de cloud, ISO/IEC 27018 – Codul de practică pentru informații personale de identificare (PII) în cloud-uri publice care acționează ca procesatori PII.

11.5.7 Raportul privind Evaluarea Impactului Asupra Protecției Datelor

Evaluarea opțiunilor de tratare/gestionare a riscurilor va avea ca rezultat realizarea RAPORTULUI PRIVIND EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR, care va detalia:

- descriere a operațiunilor de prelucrare propuse și a datelor personale implicate;
- Scopurile prelucrării incluzând, după caz, interesul legitim al operatorului de date cu caracter personal astfel cum este definit în GDPR;
- evaluare a necesității și proporționalității prelucrării în raport de scop;
- Rezultatele evaluării riscurilor la adresa drepturilor și libertăților persoanei vizate ;
- Recomandarea pentru acceptare sau tratament la adresa fiecărui risc;
- Prioritatea riscurilor la tratament/gestionare;
- Titularii riscurilor și punctul de vedere al acestora;
- Opțiunea de tratare/gestionare recomandată;
- Măsurile ce trebuie implementate;
- Responsabilitatea pentru acțiunile identificate;
- Intervalurile de timp pentru acțiuni;
- Nivelele de risc rezidual după ce măsurile au fost implementate.

11.5.8 Obținerea acordului managementului pentru riscurile reziduale

În fiecare etapă a procesului de evaluare a impactului privind protecția datelor, conducerea va fi informată cu privire la progresele și deciziile luate, inclusiv a aproba riscurile reziduale propuse a fi acceptate.

Conducerea va aproba raportul de evaluare a impactului protecției datelor și va lua în considerare în ce măsură raportul ar trebui să fie făcut public, fie în întregime, fie sub formă de rezumat.

În plus față de aprobarea generală a conducerii, acceptarea sau tratarea fiecărui risc trebuie aprobată de către titularul riscului respectiv.

11.5.9 Consultarea prealabilă a Autorității de Supraveghere

În eventualitatea în care evaluarea impactului asupra protecției datelor indică un nivel ridicat de risc chiar dacă sunt implementate măsurile identificate pentru tratare/gestionare, GDPR indică în mod expres obligația de consultare a Autorității de Supraveghere înainte de a se realiza orice prelucrare. În acest scop, trebuie transmise următoarele informații către Autoritatea de Supraveghere (A.N.S.P.D.C.P.):

a. dacă este cazul, responsabilitățile respective ale operatorului, ale operatorilor asociați și ale persoanelor împuternicite de operator implicate în activitățile de prelucrare, în special pentru prelucrarea în cadrul unui grup de întreprinderi;
b. scopurile și mijloacele prelucrării preconizate;
c. măsurile și garanțiile prevăzute pentru protecția drepturilor și libertăților persoanelor vizate, în conformitate cu GDPR;
d. dacă este cazul, datele de contact ale responsabilului cu protecția datelor (DPO);
e. evaluarea impactului asupra protecției datelor (raportul); și
f. orice alte informații solicitate de autoritatea de supraveghere.

Autoritatea de Supraveghere are un termen de 8 săptămâni (care poate fi prelungit cu încă 6 săptămâni) ca să ofere consiliere, în scris, în privința prelucrării propuse și, dacă este necesar, să ofere instrucțiuni în legătură cu măsurile necesare pentru ca prelucrarea să fie conformă cu GDPR. Autoritatea de Supraveghere are dreptul de a suspenda aceste perioade până obține informațiile pe care le-a solicitat în scopul consultării.

11.5.10 Implementarea acțiunilor de tratare/gestionare a riscurilor

Odată ce planul de tratare/gestionare a riscurilor a fost aprobat, acțiunile necesare ar trebui urmărite și realizate ca parte a derulării zilnice a proiectului.

În cazul în care acțiunile sunt întârziate sau nu pot fi finalizate, implicațiile acestora asupra protecției datelor personale implicate trebuie evaluate de către conducere și trebuie luată o decizie cu privire la ceea ce trebuie făcut în continuare.

Dacă riscul netratat este suficient de grav, acest lucru poate avea un impact semnificativ asupra viabilității proiectului din punct de vedere al conformității și ar trebui să se solicite sfaturi de la responsabilul cu protecția datelor - DPO și / sau autoritatea de supraveghere.

11.5.11 Monitorizarea și raportarea riscurilor

În cadrul implementării noilor mijloace de tratare a riscurilor și al menținerii celor existente, vor fi identificați indicatori-cheie de performanță care vor permite măsurarea succesului acestor mijloace de tratare/gestionare în abordarea și diminuarea riscurilor relevante.

Acești indicatori vor fi raportați în mod regulat și vor fi furnizate informații referitoare la tendințele observate astfel încât situațiile de excepție să poată fi identificate și tratate în cadrul procesului de revizuire.

12. ÎNCALCAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL

12.1 Ce este o încălcare de securitate a datelor cu caracter personal?

12.1.1 Definiție

Prin *"breșă sau încălcare de securitate a datelor cu caracter personal"* se înțelege o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, deteriorarea sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea.

"Distrugerea" datelor cu caracter personal înseamnă că datele nu mai există sau există într-o formă care este de niciun folos pentru operator.

Exemplu

Un exemplu de pierdere a datelor personale poate include cazul în care un dispozitiv care conține o copie a bazei de date a clienților a fost pierdut sau furat. Un alt exemplu de pierdere poate fi cazul în care singura copie a unui set de date personale a fost criptată prin ransomware sau a fost criptată de către operator folosind o cheie care nu mai este în posesia sa.

"Deteriorarea" înseamnă că datele cu caracter personal au fost modificate, corupte sau nu mai sunt complete.

"Pierderea" datelor cu caracter personal poate fi interpretată în sensul în care datele ar putea să existe, dar operatorul a pierdut controlul sau accesul la acestea sau nu le mai are în posesia sa.

Prelucrarea neautorizată sau ilegală poate include divulgarea datelor cu caracter personal către destinatari care nu sunt autorizați să primească (sau să acceseze) datele sau orice altă formă de procesare care încalcă RGPD.

12.1.2 Tipuri de încălcări a securității datelor cu caracter personal

Conform îndrumărilor WP29, încălcările pot fi clasificate în funcție de următoarele trei principii bine cunoscute privind securitatea informațiilor:

- "încălcarea confidențialității" - în cazul în care există divulgare neautorizată sau accidentală a datelor cu caracter personal sau acces neautorizat la acestea.
- "încălcarea integrității" - în cazul în care există o modificare neautorizată sau accidentală a datelor cu caracter personal.
- "încălcarea disponibilității" - în cazul în care există o pierdere accidentală sau neautorizată a accesului sau distrugere a datelor cu caracter personal.

De asemenea, trebuie remarcat faptul că, în funcție de circumstanțe, o încălcare se poate referi la confidențialitatea, integritatea și disponibilitatea datelor personale în același timp, precum și la orice combinație a acestora.

Exemplu

Exemple de încălcări/pierderi ale disponibilității includ situații în care datele au fost șterse fie accidental, fie de către o persoană neautorizată sau, în exemplul datelor criptate, cheia de decriptare a fost pierdută. În cazul în care operatorul nu poate restabili accesul la date, de exemplu, dintr-o copie de rezervă, atunci aceasta este considerată ca o pierdere permanentă de disponibilitate.

Se poate pune întrebarea dacă o pierdere temporară a disponibilității datelor cu caracter personal ar trebui considerată o încălcare și dacă este cazul să fie notificată.

Articolul 32 din GDPR, "Securitatea prelucrării", explică faptul că, atunci când se implementează măsuri tehnice și organizatorice pentru a asigura un nivel de securitate adecvat riscurilor, ar trebui să se ia în considerare, printre altele, *"capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și reziliența sistemelor și serviciilor de procesare"* și *"capacitatea de a restabili disponibilitatea și accesul la datele cu caracter personal în timp util în cazul unui incident fizic sau tehnic"*.

Prin urmare, un incident de securitate care dă naștere unei indisponibilități temporare a unor date cu caracter personal este de asemenea un tip de încălcare, deoarece lipsa accesului la date poate avea un impact semnificativ asupra drepturilor și libertăților persoanelor fizice.

Pentru a fi clar ce intră și ce nu intră în sfera definiției încălcării de securitate a datelor cu caracter personal, cazul în care datele cu caracter personal nu sunt disponibile din cauza efectuării unei întreținere planificate a sistemului nu reprezintă o "încălcare a securității", astfel cum este definită la articolul 4 alineatul (12).

Aceasta înseamnă că, ca și în cazul pierderii sau distrugerii permanente a datelor cu caracter personal, o încălcare care implică pierderea temporară a disponibilității trebuie documentată în conformitate cu articolul 33 alineatul (5). Acest lucru îl

ajută pe operator să demonstreze responsabilitatea față de autoritatea de supraveghere ANSPDCP, care poate solicita aceste înregistrări.

Cu toate acestea, în funcție de circumstanțele încălcării, se poate impune sau nu notificarea autorității de supraveghere și comunicarea către persoanele afectate.

Operatorul va trebui să evalueze probabilitatea și gravitatea impactului asupra drepturilor și libertăților persoanelor fizice ca urmare a lipsei de date cu caracter personal. În conformitate cu Articolul 33, operatorul va trebui să notifice ANSPDCP, cu excepția cazului în care este puțin probabil ca încălcarea să ducă la un risc pentru drepturile și libertățile persoanelor. Desigur, acest lucru va trebui evaluat de la caz la caz.

Trebuie remarcat faptul că, deși o pierdere a disponibilității sistemelor operatorului poate fi doar temporară și nu poate avea un impact asupra persoanelor, este important ca operatorul să ia în considerare toate consecințele posibile ale unei încălcări, deoarece este posibil să fie nevoie de notificare pentru alte motive.

12.1.3 Posibilele consecințe ale încălcării securității datelor cu caracter personal

O încălcare poate avea o serie de efecte adverse semnificative asupra persoanelor, ceea ce poate duce la daune fizice, materiale sau nemateriale. RGPD explică faptul că acestea pot include pierderea controlului asupra datelor personale, limitarea drepturilor asupra lor, discriminarea, furtul de identitate sau fraudare, pierderi financiare, reverse-engineering asupra datelor pseudonimizate, deteriorarea reputației și pierderea confidențialității datelor cu caracter personal protejate prin secret profesional. De asemenea, poate include orice alt dezavantaj economic sau social important pentru acele persoane.

Exemplu

Atacul de tip ransomware ar putea duce la pierderea temporară a disponibilității, dacă datele pot fi restabilite din copia de rezervă. Cu toate acestea, a apărut o intruziune a rețelei și ar putea fi necesară notificarea în cazul în care incidentul este calificat drept încălcare a confidențialității (adică datele personale sunt accesate de atacator), ceea ce reprezintă un risc pentru drepturile și libertățile persoanelor. O pierdere de disponibilitate poate apărea, de asemenea, în cazul în care a existat o întrerupere semnificativă a serviciului normal al unei organizații, de exemplu, în cazul unei întreruperi a alimentării cu energie sau al unui atac de tip denial-of-service, ceea ce face ca datele personale să fie indisponibile.

În consecință, RGPD solicită operatorului să notifice o încălcare către autoritatea de supraveghere competentă, cu excepția cazului în care este puțin probabil ca aceasta să ducă la riscul apariției unor astfel de efecte adverse. În cazul în care există un risc probabil ridicat de apariție a

acestor efecte adverse, GDPR cere operatorului să comunice încălcarea persoanelor afectate de îndată ce este posibil în mod rezonabil.

Dacă operatorul nu notifică autorității de supraveghere sau persoanelor vizate o încălcare a datelor, chiar dacă sunt îndeplinite cerințele articolelor 33 și/sau 34 din GDPR, **atunci autoritatea de supraveghere trebuie să ia în considerare toate măsurile corective de care dispune, care includ o amendă administrativă corespunzătoare, însoțită sau nu de o măsură corectivă în temeiul articolului 58 alineatul (2).**

De asemenea, este important să se țină seama de faptul că, în unele cazuri, nerespectarea unei încălcări ar putea dezvălui fie absența măsurilor de securitate existente, fie o inadecvare a măsurilor de securitate existente. În acest caz, autoritatea de supraveghere va avea, de asemenea, posibilitatea de a emite sancțiuni pentru necomunicarea sau comunicarea încălcării (articolele 33 și 34), pe de o parte, și absența unor măsuri de securitate (Articolul 32), pe de altă parte, întrucât acestea reprezintă două încălcări distincte.

12.2 Evaluarea riscului

Deși RGPD introduce obligația de notificare a unei încălcări, nu este o cerință în toate cazurile:

- Este necesară notificarea către autoritatea de supraveghere competentă, cu excepția cazului în care este puțin probabil ca o încălcare să ducă la **un risc** pentru drepturile și libertățile persoanelor.
- Comunicarea unei încălcări către persoana vizată este necesară numai acolo unde este posibil ca aceasta să ducă la **un risc ridicat** pentru drepturile și libertățile sale.

Acest lucru înseamnă că, imediat după ce a luat cunoștință de o încălcare, este extrem de important ca operatorul să nu urmărească numai limitarea incidentului, dar ar trebui să evalueze și riscul care ar putea rezulta din acesta.

12.2.1 Criterii de luat în considerație în evaluarea riscului

Considerentele 75 și 76 din RGPD sugerează că, în general, atunci când se evaluează riscul, trebuie luate în considerație atât probabilitatea, cât și severitatea (impactul) riscului pentru drepturile și libertățile persoanelor vizate. Se afirmă, de asemenea, că riscul ar trebui evaluat pe baza unei evaluări obiective.

Trebuie remarcat faptul că evaluarea riscului pentru drepturile și libertățile cetățenilor ca urmare a unei încălcări are un accent diferit față de riscul luat în

considerare într-o DPIA. DPIA ia în considerație atât riscurile prelucrării datelor conform planificării, cât și riscurile în cazul unei încălcări.

Prin urmare, Grupul de Lucru WP29, prin opiniile sale recomandă ca evaluarea să țină seama de următoarele criterii:

- Tipul de încălcare
- Natura, sensibilitatea și volumul datelor cu caracter personal
- Ușurința în identificarea indivizilor
- Severitatea consecințelor asupra persoanelor
- Caracteristicile speciale ale persoanei vizate
- Caracteristicile speciale ale operatorului de date
- Numărul persoanelor afectate
- Puncte generale

Atunci când evaluează riscul care ar putea rezulta dintr-o încălcare, operatorul ar trebui să ia în considerare o combinație a gravității impactului potențial asupra drepturilor și libertăților persoanelor și a probabilității apariției acestora.

În mod evident, în cazul în care consecințele unei încălcări sunt mai severe, riscul este mai mare și, în mod similar, în cazul în care probabilitatea apariției acestora este mai mare, riscul este, de asemenea, sporit. În caz de îndoială, operatorul ar trebui să notifice ANSPDCP.

Exemplu

DPIA sugerează că utilizarea propusă a unui anumit produs software de securitate pentru a proteja datele personale este o măsură adecvată pentru a asigura un nivel de securitate adecvat riscului pe care l-ar putea prezenta în mod individual pentru persoanele vizate. Cu toate acestea, dacă o vulnerabilitate devine ulterior cunoscută, acest lucru ar schimba caracteristica software-ului de a fi adecvat pentru a limita riscul pentru datele cu caracter personal protejate și, prin urmare, va trebui să fie reevaluat ca parte a unui DPIA nou.

O vulnerabilitate a produsului este ulterior exploatată și apare o încălcare. Operatorul ar trebui să evalueze circumstanțele specifice ale încălcării, datele afectate și nivelul potențial de impact asupra persoanelor, precum și probabilitatea ca acest risc să se materializeze.

12.3 Notificarea Autorității de Supraveghere

12.3.1 Cine este Autoritatea de Supraveghere?

Autoritatea de supraveghere pentru aplicarea RGPD în România este:

Denumire:	**Autoritatea Națională pentru Supravegherea Prelucrării Datelor cu Caracter Personal - ANSPDCP**
Adresă:	B-dul G-ral. Gheorghe Magheru 28-30 Sector 1, cod postal 010336 Bucuresti, Romania
Telefon:	+40.318.059.211 +40.318.059.212
Fax:	+40.318.059.602
Email:	anspdcp@dataprotection.ro

12.3.2 Când trebuie să notificăm Autoritatea de Supraveghere?

Trebuie să raportați o încălcare notificabilă către ANSPDCP fără întârzieri nejustificate, dar NU MAI TÂRZIU DE 72 DE ORE după ce v-ați dat seama de ea. Dacă vă ia mai mult de 72 de ore, trebuie să justificați întârzierea notificării.

12.3.3 Ce informații trebuie să conțină o Notificarea către autoritatea de supraveghere?

Când raportați o încălcare, Articolul 33 alineatul (3) prevede că, cel puțin, trebuie notificate următoarele:

a) descrierea naturii încălcării 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;
b) comunicarea numelui și a datelor de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
c) descrierea consecințelor probabile ale încălcării securității datelor cu caracter personal;
d) descrierea măsurilor 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 sale efecte negative.

12.3.4 Cum notificăm Autoritatea de Supraveghere?

Formularul pentru notificarea breşelor de securitate către ANSPDCP poate fi găsit aici https://www.dataprotection.ro/?page=pagina_formular_679

Ulterior completării şi semnării în format electronic, formularul trebuie trimis către: brese@dataprotection.ro.

Atenție! Formularele care nu sunt semnate electronic nu vor fi luate în considerare!

12.3.5 Notificarea în faze

Articolul 33 alineatul (4) din RGPD prevede: *Atunci când și în măsura în care nu este posibil să se furnizeze informațiile în același timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate.*

Aceasta înseamnă că RGPD recunoaște că operatorii nu vor avea întotdeauna toate informațiile necesare cu privire la o încălcare în termen de 72 de ore de la conștientizarea acesteia, deoarece detaliile complete ale incidentului nu pot fi întotdeauna disponibile de la început.

Ca atare, permite o notificare în etape.

Este mult mai probabil ca acest tip de notificare să apară în cazul unor încălcări mai complexe, cum ar fi unele tipuri de incidente de securitate cibernetică, în care, spre exemplu, ar putea fi necesară o investigație legală aprofundată pentru a stabili pe deplin natura încălcării și măsura în care datele personale au fost compromise. În consecință, în multe cazuri, operatorul va trebui să facă mai multe investigații și să revină cu informații suplimentare ulterior. Acest lucru este permis, în cazul în care operatorul explică ce motive are pentru întârziere, în conformitate cu articolul 33 alineatul (1).

12.3.6 Notificarea întârziată

Articolul 33 alineatul (1) din RGPD precizează că, în cazul în care notificarea către autoritatea de supraveghere nu se face în termen de 72 de ore, aceasta este trebuie însoțită de motivarea întârzierii. Această posibilitate, împreună cu noțiunea de notificare în etape, recunoaște că un operator nu poate întotdeauna să fie în măsură să notifice o încălcare în termenul legal și că poate fi admisă o notificare întârziată.

12.3.7 Situații în care notificarea nu se impune

Articolul 33 alineatul (1) din RGPD precizează că încălcările pentru care *"nu există probabilitate de risc pentru drepturile și libertățile persoanelor fizice"* nu impun

notificarea autorității de supraveghere. Un exemplu ar putea fi cazul în care datele cu caracter personal sunt deja disponibile în mod public și o divulgare a acestor date nu constituie un risc probabil pentru individ.

12.3.8 Ce se întâmplă dacă nu notificăm Autoritatea Națională?

Nerespectarea notificării unei încălcări, atunci când este necesar, poate conduce la o **amendă** semnificativă de până la **10 milioane de euro** sau 2 % **din cifra de afaceri globală.**

Amenda poate fi combinată cu alte sancțiuni ale ANSPDCP în conformitate cu articolul 58 GDPR. Prin urmare, este important ca operatorul să implementeze un proces bine documentat și chiar testat de raportare a încălcărilor care să vă asigure detectarea și notificarea la timp a unei încălcări precum și să furnizeze detaliile necesare.

12.4 Notificarea Persoanelor Vizate

12.4.1 Informarea persoanelor vizate

Conform Articolul 34 alineatul (1) din RGPD: *În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.*

Notificarea către autoritatea de supraveghere este obligatorie, cu excepția cazului în care este puțin probabil să existe un risc pentru drepturile și libertățile persoanelor ca urmare a încălcăril.

În plus, în cazul în care există un risc ridicat pentru drepturile și libertățile persoanelor ca urmare a unei încălcări, persoanele vizate trebuie de asemenea să fie informate. Prin urmare, pragul de comunicare a unei încălcări persoanelor vizate este mai ridicat decât pentru notificarea autorităților de supraveghere și nu este necesar ca toate încălcările să fie comunicate persoanelor vizate.

GDPR afirmă că comunicarea unei încălcări persoanelor fizice trebuie făcută "fără întârzieri nejustificate", ceea ce înseamnă cât mai curând posibil. Obiectivul principal al comunicării către persoanele fizice este furnizarea de informații specifice despre măsurile pe care ar trebui să le ia pentru a se proteja.

12.4.2 Ce informații trebuie să fie puse la dispoziție?

Conform Articolul 34 alineatul (2) din RGPD: În informarea transmisă persoanei vizate prevăzută la alineatul (1) din prezentul articol se include o descriere într-un limbaj clar și simplu a naturii încălcării securității datelor cu caracter personal,

precum și cel puțin informațiile și măsurile menționate la articolul 33 alineatul (3) literele (b), (c) și (d).

Conform acestei prevederi, operatorul ar trebui să furnizeze cel puțin următoarele informații:

- o descriere a naturii încălcării;
- numele și datele de contact ale responsabilului cu protecția datelor sau ale altui punct de contact;
- o descriere a consecințelor probabile ale încălcării; și
- o descriere a măsurilor luate sau propuse a fi luate de către operator pentru a remedia încălcarea, inclusiv, dacă este cazul, măsuri de atenuare a posibilelor sale efecte adverse.

De asemenea, operatorul ar trebui să ofere, dacă este cazul, suport specific persoanelor fizice pentru a se proteja de posibilele consecințe negative ale încălcării, cum ar fi resetarea parolelor în cazul în care credențialele lor de acces au fost compromise. Din nou, operatorul poate alege să furnizeze informații în plus față de ceea ce este strict necesar conform legii.

12.4.3 Contactarea persoanelor

În principiu, încălcarea ar trebui comunicată direct persoanelor vizate, cu excepția cazului în care acest lucru ar implica un efort disproporționat. În acest caz, trebuie să existe o comunicare publică sau o măsură similară prin care persoanele vizate să fie informate în mod la fel de eficient (articolul 34 alineatul (3) litera (c)).

Atunci când se comunică o încălcare persoanelor vizate ar trebui utilizate mesaje dedicate și comunicarea nu ar trebui trimisă împreună cu alte informații, cum ar fi actualizări regulate, buletine de știri, newsletters sau mesaje standard. Aceasta asigură claritatea și transparența comunicării încălcării.

Exemple de metode de comunicare transparentă includ mesajele directe (de exemplu, e-mail, SMS, mesaj direct), bannere de site-uri proeminente sau notificări, comunicări poștale și anunțuri proeminente în presa scrisă. O notificare limitată doar într-un comunicat de presă sau într-un blog corporativ nu ar fi un mijloc eficient de comunicare a unei încălcări.

Grupul de Lucru WP29 recomandă operatorilor să aleagă un mijloc care maximizează șansa de a comunica în mod corespunzător încălcarea tuturor persoanelor afectate. În funcție de circumstanțe, acest lucru poate impune ca operatorul să utilizeze mai multe metode de comunicare, spre deosebire de utilizarea unui singur canal de contact.

De asemenea, operatorii trebuie să se asigure că comunicarea este accesibilă în formate alternative adecvate și limbi relevante pentru a se asigura că persoanele

sunt în măsură să înțeleagă informațiile pe care le transmit. De exemplu, atunci când se comunică o încălcare unei persoane, limba utilizată în timpul desfășurării normale a afacerii cu destinatarul va fi, în general, adecvată.

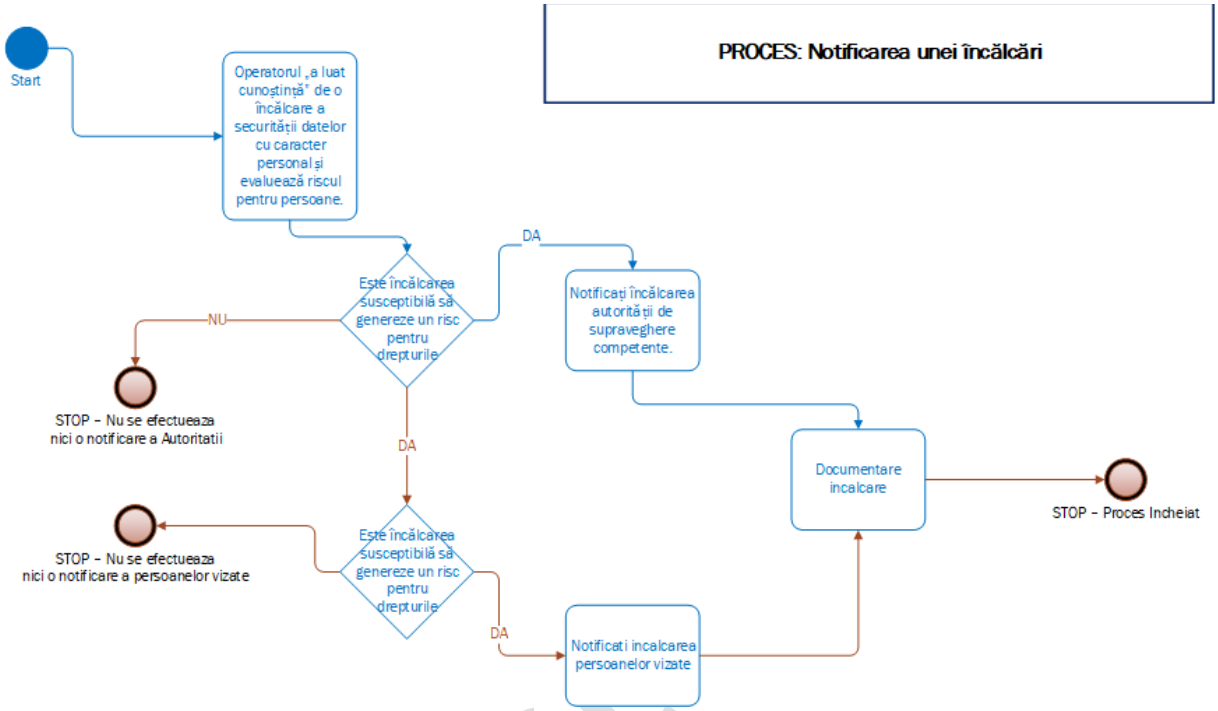
12.4.4 Situații în care comunicarea către persoanele vizate nu este necesară

Articolul 34 alineatul (3) prevede trei condiții care, dacă sunt îndeplinite, înlătură necesitatea de comunicare a breșelor către persoanele vizate. Acestea sunt:

- Operatorul a aplicat măsuri tehnice și organizatorice adecvate pentru a proteja datele cu caracter personal înainte de încălcare, în special acele măsuri care fac ca datele personale să fie incomprehensibile oricărei persoane care nu este autorizată să le acceseze. Aceasta ar putea include, de exemplu, protejarea datelor cu caracter personal prin criptare de ultimă oră sau prin tokenizare.
- Imediat după o încălcare, operatorul a luat măsuri pentru a se asigura că riscul ridicat pentru drepturile și libertățile persoanelor nu mai este posibil să se materializeze. De exemplu, în funcție de circumstanțele cazului, operatorul poate să fi identificat imediat și să ia măsuri împotriva persoanei care a accesat date cu caracter personal înainte de a putea face ceva cu ele. Trebuie să se țină seama în continuare de posibilele consecințe ale încălcării confidențialității, din nou, în funcție de natura datelor în cauză.
- Ar presupune un efort disproporționat de a contacta indivizii, poate chiar în cazul în care datele lor de contact au fost pierdute ca urmare a încălcării sau nu erau cunoscute de la început. De exemplu, depozitul unui birou de statistică e inundat, iar documentele care conțin date cu caracter personal au fost stocate numai pe suport de hârtie. În schimb, operatorul trebuie să facă o comunicare publică sau să ia o măsură similară, prin care indivizii sunt informați într-o manieră la fel de eficientă. În cazul eforturilor disproporționate, ar putea fi avute în vedere și aranjamentele tehnice pentru a face disponibile informații la cerere, care ar putea fi utile pentru acele persoane care pot fi afectate de o încălcare, dar pe care operatorul nu le poate contacta altfel.

12.5 Procesul de notificare a unei încalcări

O digramă de proces pentru toate elementele descrise în capitolul prezent se regăsește în figura următoare:



13. REMEDII, RĂSPUNDERE, PENALITĂȚI

Amenzile prevăzute de GDPR (și care se aplică în mod direct în România) au fost *crescute în mod considerabil* față de vechea legislație, până la un maximum de 20 milioane EURO sau 4% din cifra totală de afaceri la nivel global.

În același timp, puterile de investigație și control ale autorității de supraveghere au fost extinse. Legiuitorul național a considerat necesar să întărească puterile autorității de supraveghere pentru a monitoriza și asigura conformarea la RGPD, precum și să introducă sancțiuni semnificative pentru încălcare pentru a asigura o protecție eficientă a datelor personale în cadrul UE.

13.1 Atribuțiile Autorității de Supraveghere

Atribuțiile Autorității de Supraveghere au fost în mod considerabil *extinse* și sunt descrise în detaliu în Legea nr. 129/2018 și RGPD.
Conform articolului 57 GDPR, aceste atribuții pot fi clasificate în două categorii:

a) Atribuții care servesc protecției imediate a drepturilor și libertăților

persoanelor vizate, precum monitorizarea și punerea în aplicarea a Regulamentului; și

b) Atribuții care servesc indirect acestui scop, precum promovarea publică a protecției datelor, furnizarea de informații și îndrumări pentru diferite persoane interesate sau cooperarea cu alte autorități de supraveghere.

13.2 Puterile de investigație ale Autorității de Supraveghere

Potrivit articolului 58 alin. (1) lit. a)-f) din RGPD, fiecare autoritate de supraveghere națională va avea următoarele puteri de investigație:

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;
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.

13.3 Competențe coercitive ale Autorității de Supraveghere

Potrivit Art. 58 alin. (2) din RGPD, fiecare autoritate de supraveghere are toate următoarele competențe corective:

a) de a emite avertizări în atenția unui operator sau a unei persoane împuternicite de operator cu privire la posibilitatea ca operațiunile de prelucrare prevăzute să încalce dispozițiile prezentului regulament;
b) de a emite mustrări adresate unui operator sau unei persoane împuternicite de operator în cazul în care operațiunile de prelucrare au încălcat dispozițiile prezentului regulament;

c) de a da dispoziții operatorului sau persoanei împuternicite de operator să respecte cererile persoanei vizate de a-și exercita drepturile în temeiul prezentului regulament;
d) de a da dispoziții operatorului sau persoanei împuternicite de operator să asigure conformitatea operațiunilor de prelucrare cu dispozițiile prezentului regulament, specificând, după caz, modalitatea și termenul-limită pentru aceasta;
e) de a obliga operatorul să informeze persoana vizată cu privire la o încălcare a protecției datelor cu caracter personal;
f) de a impune o limitare temporară sau definitivă, inclusiv o interdicție asupra prelucrării;
g) de a dispune rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării, în temeiul articolelor 16, 17 și 18, precum și notificarea acestor acțiuni destinatarilor cărora le-au fost divulgate datele cu caracter personal, în conformitate cu articolul 17 alineatul (2) și cu articolul 19;
h) de a retrage o certificare sau de a obliga organismul de certificare să retragă o certificare eliberată în temeiul articolul 42 și 43 sau de a obliga organismul de certificare să nu elibereze o certificare în cazul în care cerințele de certificare nu sunt sau nu mai sunt îndeplinite;
i) de a impune amenzi administrative în conformitate cu articolul 83, în completarea sau în locul măsurilor menționate la prezentul alineat, în funcție de circumstanțele fiecărui caz în parte;
j) de a dispune suspendarea fluxurilor de date către un destinatar dintr-o țară terță sau către o organizație internațională.

13.4 Competențe de autorizare și consiliere ale Autorităților de Supraveghere

Potrivit Art. 58 alin. (3) din RGPD, 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
j) de a aproba reguli corporatiste obligatorii în conformitate cu articolul 47.

13.5 Procedura de control a ANSPDCP

13.5.1 Cine face controlul?

Controlul în domeniul RGPD, efectuat de autoritate, se numeşte **inspecţie.** În cadrul ANSPDCP, vor exista persoane cu funcţii de control, denumit personal de control. Personalul de control va fi numit de către preşedintele ANSPDCP.

13.5.2 Ce poate controla personalul de control?

Inspecţiile pot fi de două feluri:

- Anunțată – când entitatea va primi înștiințare prealabilă despre inspecție
- Inopinantă – când entitatea se va trezi cu personalul de control la sediul/locul unde își desfășoară activitatea.

Drepturile personalului de control:

- să ceară şi să obţină de la operator şi persoana împuternicită de operator, precum şi, după caz, de la reprezentantul acestora, la faţa locului şi/sau în termenul stabilit, orice informaţii şi documente, indiferent de suportul de stocare,
- să ridice copii de pe acestea, să aibă acces la oricare dintre incintele operatorului şi persoanei împuternicite de operator, precum şi să aibă acces şi să verifice orice echipament, mijloc sau suport de stocare a datelor, necesare desfăşurării investigaţiei, în condiţiile legii.

13.5.3 Putem împiedica în vreun fel controlul?

În situaţia în care personalul de control este împiedicat în orice mod în exercitarea atribuţiilor prevăzute la alin. (2), Autoritatea naţională de supraveghere poate solicita autorizarea judiciară dată prin încheiere de către preşedintele Curţii de Apel Bucureşti sau de către un judecător delegat de acesta.
O copie a autorizaţiei judiciare se comunică obligatoriu entităţii controlate înainte de începerea investigaţiei.

Cererea de autorizare se judecă în camera de consiliu, fără citarea părţilor.
Judecătorul se pronunţă asupra cererii de autorizare în termen de cel mult 48 de ore de la data înregistrării cererii. Încheierea se motivează şi se comunică Autorităţii naţionale de supraveghere şi entităţii controlate în termen de cel mult 48 de ore de la pronunţare.

În cazul în care investigaţia trebuie desfăşurată, inclusiv simultan, în mai multe spaţii deţinute de către entitatea controlată, Autoritatea naţională de supraveghere va introduce o singură cerere, instanţa pronunţându-se printr-o încheiere în care se vor indica spaţiile în care urmează să se desfăşoare investigaţia.

Cererea de autorizare trebuie să cuprindă toate informaţiile de natură să justifice investigaţia, iar judecătorul sesizat este ţinut să verifice dacă cererea este întemeiată.
Încheierea prevăzută la alin. (3) poate fi atacată cu contestaţie la Înalta Curte de Casaţie şi Justiţie, în termen de 72 de ore de la comunicarea acesteia potrivit alin.
Contestaţia nu este suspensivă de executare.

13.6 Plângerile persoanelor vizate

Orice persoană vizată care consideră că prelucrarea datelor sale cu caracter personal încalcă prevederile legale în vigoare are dreptul de a depune plângere la Autoritatea naţională de supraveghere, în special în cazul în care reşedinţa sa obişnuită, locul său de muncă sau presupusa încălcare se află sau, după caz, are loc pe teritoriul României. Plângerea poate fi depusă inclusiv prin mijloacele electronice de comunicare.
Plângerea poate fi depusă de:

- personal de persoana vizată;
- prin împuternicitul persoanei vizate;
- de către un mandatar al persoanei vizate;
- de către un organism, organizaţie, asociaţie sau fundaţie fără scop patrimonial care activează în domeniul protecţiei drepturilor şi libertăţilor persoanelor vizate în ceea ce priveşte protecţia datelor lor cu caracter

personal.

Dacă ANSPDCP consideră că plângerea nu este completă/insuficientă, va informa, în termen de 45 zile de la înregistrarea plângerii, persoana vizată despre acest aspect şi îi va solicita să completeze plângerea cu informaţiile şi documentele necesare. Un nou termen de 45 zile va începe să curgă de la data completării cererii.

ANSPDCP a considerat plângerea ca fiind admisibilă, va informa persoana vizată despre evoluţia sau rezultatul investigaţiei întreprinse (care poate fi de admitere a plângerii sau de respingere a acesteia).

Dacă este necesară efectuarea unei investigaţii mai amănunţite sau coordonarea cu alte autorităţi de supraveghere, ANSPDCP informează persoana vizată în legătură cu evoluţia investigaţiei, din 3 în 3 luni, până la finalizarea acesteia. Rezultatul investigaţiei se aduce la cunoştinţa persoanei vizate în termen de cel mult 45 de zile de la finalizarea acesteia.

Dacă nu sunt respectate dispoziţiile anterior menţionate, persoana vizată se poate adresa secţiei de contencios administrativ a tribunalului competent, după parcurgerea procedurii prealabile prevăzute de Legea contenciosului administrativ nr. 554/2004. Recursul se judecă de curtea de apel competentă, instanţele competente fiind în toate cazurile cele din România.

13.7 Sancțiunile

Potrivit RGPD, amenzile sunt: **mustrarea** şi **amenda.**

De asemenea, în anumite cazuri, **ANSPDCP poate emite avertizări**.

Amenda contravenţională de până la 10 000 000 EUR sau, în cazul unei întreprinderi, de până la 2 % din cifra de afaceri pentru încălcarea:

- obligaţiilor operatorului şi ale persoanei împuternicite în conformitate cu articolele 8,11, 25-39,42 şi 43 RGPD;
- obligaţiile organismului de certificare în conformitate cu articolele 42 şi 43 RGPD;
- obligaţiile organismului de monitorizare în conformitate cu articolul 41 alineatul (4) RGPD.

Amenda contravenţională de până la 20 000 000 EUR sau, în cazul unei întreprinderi, de până la 4 % din cifra de afaceri pentru încălcarea:

- principiile de bază pentru prelucrare, inclusiv condiţiile privind consimţământul, în conformitate cu articolele 5,6, 7 şi 9 RGPD;
- drepturile persoanelor vizate în conformitate cu articolele 12-22 RGPD;

- transferurile de date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională, în conformitate cu articolele 44-49 RGPD;
- orice obligații în temeiul legislației naționale adoptate;
- nerespectarea unui ordin sau a unei limitări temporare sau definitive asupra prelucrării, sau a suspendării fluxurilor de date, emisă de către autoritatea de supraveghere;
- încălcarea unui ordin emis de autoritatea de supraveghere în conformitate cu articolul 58 alineatul (2) GDPR.

EXCEPȚIA DE LA CELE DE MAI SUS O CONSTITUIE AUTORITĂȚILE ȘI ORGANISMELE PUBLICE ASTFEL:

Conform Art. 14 ale Legii 190/2018, Amenda maximă care se poate aplica, în cazul în care autoritățile și organismele publice nu au dus la îndeplinire în totalitate măsurile de remediere este de 200.000 lei.

Pentru a stabili dacă se va da un avertisment sau o amendă, sau, în cazul unei amenzi, pentru stabilirea cuantumului acesteia, se vor avea în vedere următoarele:

- natura, gravitatea și durata încălcării, ținându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum și de numărul persoanelor vizate afectate și de nivelul prejudiciilor suferite de acestea;
- dacă încălcarea a fost comisă intenționat sau din neglijență;
- acțiunile întreprinse pentru reducerea prejudiciului pentru persoana vizată;
- garadul de responsabilitate:
- eventualele încălcări anterioare relevante:
- Gradul de cooperare cu autoritatea de supraveghere pentru a remedia încălcarea și a atenua posibilele efecte negative ale încălcării;
- categoriile de date cu caracter personal afectate de încălcare
- modul în care încălcarea a fost adusă la cunoștința autorității de supraveghere. în special dacă și în ce măsură operatorul sau persoana împuternicită de operator a notificat încălcarea;
- aderarea la coduri de conduită aprobate;
- 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.

13.7.1 În cât timp se pot aplică sancțiunile?

Sancţiunile pot fi aplicate în termenul de prescripţie de 3 ani de la data săvârşirii faptei. În cazul încălcărilor care durează în timp sau al celor constând în săvârşirea, în baza aceleiaşi rezoluţii, la intervale diferite de timp, a mai multor acţiuni sau inacţiuni, care prezintă, fiecare în parte, conţinutul aceleiaşi contravenţii, prescripţia începe să curgă de la data constatării sau de la data încetării ultimului act ori fapt săvârşit, dacă acest moment intervine anterior constatării.

Atenţie! Termenul de prescripţie se întrerupe prin efectuarea oricărui act de procedură în cazul investigat, fără să poată depăşi 4 ani de la data săvârşirii faptei. întreruperea produce efecte faţă de toţi participanţii la săvârşirea respectivei încălcări.