Ghid GDPR
pentru ONG-uri

Material publicat în cadrul proiectului „Evaluarea impactului legislației GDPR și AML asupra sectorului ONG din România"

Program finanțat printr-un grant acordat de Romanian-American Foundation

Cuprins

I. Ce este GDPR și ce obligații generale presupune?

1. Regulamentul General privind Protecția Datelor Personale

Care este scopul GDPR: datele personale ale persoanelor fizice să fie colectate în mod limitat, transparent, responsabil și proporțional.

Cadrul legislativ:

Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date

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

2. Explicarea termenilor folosiți de GDPR

2.1 Date personale

Înseamnă orice informații privind o **persoană fizică** identificată sau identificabilă[1] („persoana vizată");

O persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale

GDPR se aplică cu privire la datele persoanelor fizice, dar chiar și când datele sunt profesionale (de exemplu numărul de telefon sau email de birou).

Datele personale se împart în:

- **Identificatori direcți:** CNP-ul, numărul de telefon mobil sau localizarea exactă a unei persoane care mă duc întotdeauna la o anumită persoană fizică.
- **Identificatori indirecți:** sunt date care de sine stătătoare nu-mi pot indica o anumită persoană (precum vârsta sau genul), dar care atunci când le asociez unei persoane deja cunoscute sau care grupate cu suficient de multe date mă ajută să

[1] Art. 4 alin. (1) GDPR.

identific unic o persoană (de exemplu, persoană de sex feminin care locuiește la etajul 5 sau o persoană cu numele de familie Ionescu că are 25 de ani).

2.2 Prelucrare[2]

Orice operațiune care implică date cu caracter personal, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, profilarea, extragerea, consultarea/vizualizarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.

De exemplu: introducerea datelor în sisteme și aplicații, colectarea datelor prin formulare sau la telefon, activități de profilare, înregistrarea unei reclamații.

Cu alte cuvinte, de fiecare dată când utilizăm în orice mod date cu caracter personal, înseamnă că prelucrăm acele date. Chiar și simpla stocare a datelor reprezintă prelucrare.

2.3 Operator de date[3]

Operator înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal. Atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern.

Operatori asociați[4]

Operatori asociați sunt doi sau mai mulți operatori care stabilesc în comun scopurile și mijloacele de prelucrare. Operatorii asociați stabilesc într-un mod transparent responsabilitățile fiecăruia în ceea ce privește îndeplinirea obligațiilor care le revin în temeiul GDPR în special în ceea ce privește exercitarea drepturilor persoanelor vizate și îndatoririle fiecăruia de furnizare a informațiilor prevăzute la articolele 13 și 14, prin intermediul unui acord între ei, cu excepția cazului și în măsura în care responsabilitățile operatorilor sunt stabilite în dreptul Uniunii sau în dreptul intern care se aplică acestora.

Persoană împuternicită de operator[5]

Persoana împuternicită de operator înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului.

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

[2] Art. 4 alin. (2) GDPR.

[3] Art. 4 alin. (7) GDPR.

[4] Art. 26 GDPR.

[5] Art. 4 și art. 28 GDPR.

respecte cerințele prevăzute de GDPR și să asigure protecția drepturilor persoanei vizate[6]

Prelucrarea efectuată de către o persoană împuternicită în numele unui operator este reglementată printr-un contract sau alt act juridic în temeiul dreptului Uniunii sau al dreptului intern care are caracter obligatoriu pentru persoana împuternicită de operator 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 și obligațiile și drepturile operatorului.

2.4 Persoana vizată

Orice persoană fizică ale cărei date personale sunt prelucrate.

Atenție! Prevederile GDPR se aplică și reprezentanților persoanelor juridice cu care interacționăm care sunt persoane fizice și deci sunt persoane vizate din perspectiva GDPR.

De exemplu: datele reprezentantului unei alte organizații partenere

2.5 Autoritatea de supraveghere

Este o autoritate publică independentă instituită de un stat membru în temeiul articolului 51 GDPR. În cazul României, autoritatea de supraveghere este **Agenția Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (https://www.dataprotection.ro/).**

3. Cum trebuie să fie colectate datele personale?

Limitat

Scopul prelucrării trebuie să fie clar stabilit de către ONG de la începutul planificării procesului de prelucrare. Astfel, atunci când se ajunge la momentul colectării, se știe exact ce date vor fi necesare a se atinge scopul.

Doar în temeiurile prevăzute de lege (conform art. 6 GDPR)

Art. 6 GDPR prevede temeiurile care permit colectarea de date personale. Astfel, înainte de începerea colectării, operatorul trebuie să identifice scopul pentru care colectează datele și temeiul care îi permite să le colecteze.

Proporțional

Odată stabilit scopul prelucrării, ONG-ul trebuie să prelucreze doar acele date de care are nevoie pentru a-și atinge scopul. Nu trebuie să se colecteze date personale în plus.

[6] Art. 28 GDPR.

Transparent

ONG-ul trebuie să informeze corect și complet persoana vizată cu privire la datele care îi sunt prelucrate, scopul prelucrării și măsurile luate pentru asigurarea securității acestor date. Informarea se face obligatoriu înaintea prelucrării.

Desigur, pentru ca informarea să fie corectă și completă trebuie ca anterior ONG-ul să definească exact scopul colectării datelor.

Responsabil

ONG-ul trebuie să cunoască și să respectele limitele colectării și principiile generale ale GDPR. De asemenea, ONG-ul trebuie să poată dovedi respectarea GDPR. De aceea toate măsurile luate la nivelul organizației trebuie documentate.

4. Obligații impuse de GDPR

4.1 Obligațiile generale impuse de GDPR oricărui operator de date personale:

A. Respectarea principiilor generale aplicabile operatorilor când prelucrează date personale[7]

Limitarea scopului prelucrării

ONG-urile pot colecta date personale doar pentru un scop bine determinat și explicat, și doar în măsura în care datele personale pe care le colectează sunt necesare pentru atingerea acelui scop.

Minimizarea datelor colectate

Să colecteze doar acele datele personale care sunt necesare pentru a atinge scopul urmărit.

Colectarea datelor în mod transparent și legal

ONG-ul trebuie să proceseze datele personale doar în baza temeiurilor prevăzute de art. 6 din Regulament (vezi Capitolul II. Ce ne dă dreptul să prelucrăm datele personale) și să dea dovadă de transparență în relația cu persoanele vizate ale căror date personale sunt colectate

Acuratețea datelor personale colectate

ONG-ul trebuie să se asigure că datele personale colectate și stocate sunt corecte și complete. Mai mult, trebuie să fie luate toate măsurile pentru identificarea celor care nu sunt corecte și rectificarea/completarea acestora.

[7] Art. 5 GDPR.

Durata limitată a stocării datelor personale colectate

Datele personale nu pot fi colectate pentru o perioadă nedeterminată. ONG-ul trebuie să se asigure că, odată ce datele personale colectate nu mai sunt necesare, aceste vor fi șterse sau distruse (dacă sunt păstrate în format fizic pe hârtie) în mod responsabil și sigur.

Integritatea și confidențialitatea datelor colectate

Datele personale trebuie prelucrate într-un mod care să asigure securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, distrugerii sau deteriorării accidentale, utilizând măsuri tehnice sau organizaționale adecvate.

Responsabilitatea operatorului de date

ONG-ul trebuie să documenteze respectarea acestor obligații prin documente doveditoare. Detaliile unei prelucrări care nu a fost documentată (pe hârtie sau în format electronic în orice formă fie e-mail, fie înregistrare etc.) vor fi foarte greu de dovedit în relația cu Autoritatea de Supraveghere.

B. Asigurarea drepturilor persoanelor ale căror date sunt prelucrate[8] (3)

Persoanele ale căror date personale sunt prelucrate au următoarele drepturi:

- Dreptul la informare
- Dreptul de acces la datele personale
- Dreptul de a fi uitat
- Dreptul la restricționarea prelucrării
- Dreptul la opoziție
- Dreptul de a depune plângere

Asigurarea în practică a acestor drepturi presupune că ONG-ul:

A. Are o procedură care prevede cum vor fi tratate cererile persoanelor vizate și care să asigure din perspectivă organizatorică un răspuns persoanei vizate. Astfel, ONG-ul trebuie să pună la dispoziția publicului un canal de comunicare cu privire la datele personale colectate și stocate

B. Are capacitatea efectivă de a da curs cererilor de exercitare a drepturilor din partea persoanelor vizate. ONG-ul trebuie să se asigure că sistemele care stochează datele permit rectificarea/ștergerea acestora și să se asigure că datele sunt stocate organizat și pot fi identificate în mod facil.

Pentru mai multe detalii despre drepturile persoanelor vizate vezi Capitolul V. Drepturile persoanelor ale căror date sunt prelucrate.

[8] Art. 12-23 GDPR.

C. Asigurarea securității datelor[9] și obligația de a notifica Autoritatea de supraveghere în cazul unui incident de securitate

ONG-ul trebuie să se asigure că sunt aplicate măsuri de securitate IT și securitate fizică. Toate mediile pe care sunt stocate date personale trebuie protejate corespunzător (de exemplu: laptop-uri, alte dispozitive de stocare digitală, dar și dulapurile în care sunt stocate dosarele cu informații) .

Exemple de măsuri de protecție pe care ONG-ul trebuie să le aibă în vedere:

- protecție antivirus pentru laptop-uri;
- actualizarea constantă a sistemelor și aplicațiilor folosite
- evaluare periodică a infrastructurii IT,
- adoptarea unei politicii de utilizare a dispozitivelor personale, parolarea dispozitivelor utilizate în mod corespunzător
- asigurarea confidențialității prin măsuri care nu permit persoanelor străine să acceseze dispozitivele etc.,
- să se asigure că în spațiile de lucru au acces doar anumite persoane sau utilizarea de încuietori pentru dulapurile unde sunt stocare dosarele cu informații cu caracter personal

4.2 Obligații specifice

GDPR prevede că în anumite cazuri speciale apar obligații specifice, recomandarea **Autorității de Supraveghere** fiind ca fiecare ONG să evalueze dacă implementarea voluntară a acestora nu îi este utilă în desfășurarea propriilor activități.

A. Numirea unui responsabil cu prelucrarea datelor personale (Data Protection Officer)[10]

GDPR prevede la art. 37 situațiile când este obligatoriu ca operatorul de date să numească un **responsabil cu protecția datelor** (*Data protection officer*, de aici încolo "**DPO**") care cunoaște obligațiile impuse de GDPR.

Este obligatoriu ca ONG-ul să numească un DPO dacă:

1. Prelucrează date cu caracter special pe scară largă sau date cu caracter personal privind condamnări penale și infracțiuni
2. Activitățile principale ale ONG-ului constau în operațiuni de prelucrare care, prin natura, domeniul de aplicare și/sau scopurile lor, necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă
3. Prelucrarea este efectuată de o autoritate sau un organism public (în cazul nostru o asociație sau fundație de utilitate publică)

[9] Art. 25 și 32 GDPR.

[10] Art. 37-39 GDPR.

Chiar și atunci când nu există obligația legală de a numi un DPO, este recomandat ca ONG-ul să aibă o persoană responsabilă cu protecția datelor personale care să asigure instruirea angajaților cu privire la standardele GDPR și politica interna a ONG-ului cu privire la prelucrarea acestor date și să ofere îndrumare atunci când ONG-ul colectează date personale cu caracter special .

Pe scurt, DPO-ul are cel puțin următoarele sarcini:

- informează și consiliază operatorul (inclusiv angajații acestuia) cu privire la obligațiile legale care le revin în domeniul protecției datelor personale
- monitorizează respectarea obligațiilor legale cu privire la protecția datelor și a politicilor operatorului
- furnizează consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia,
- este persoana de contact a ONG-ului în relația cu autoritatea de supraveghere

Persoana desemnată ca DPO poate îndeplini și alte sarcini în cadrul ONG-ului. Cu toate acestea **nu poate fi DPO o persoană care are putere de decizie la nivelul ONG-ului** (membru în consiliul director, președinte, director executiv etc.), pentru a nu intra în conflict de interese.

Pentru mai multe detalii despre DPO vezi Capitolul IV. Prelucrarea datelor personale cu caracter special, Secțiunea 2.

B. Cartografierea prelucrării de date cu caracter personal[11]

GDPR prevede la art. 30 situațiile în care operatorul de date este obligat să efectueze o cartografiere a datelor cu caracter personal prelucrate la nivelul organizației.

Conform art. 30 alin. (5) din GDPR, cartografierea este obligatorie:

- în cazul întreprinderi sau organizații cu mai mult de 250 de angajați sau
- atunci când prelucrarea este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate și nu este o prelucrare ocazională sau
- prelucrarea include categorii speciale de date (art. 9 GDPR), sau
- prelucrarea include categorii de date cu caracter personal referitoare la condamnări penale și infracțiuni (art. 10 GDPR)

Pe scurt, cartografierea presupune întocmirea unei evidențe a prelucrărilor de date personale de la nivelul organizației și se referă la păstrarea informațiilor ce privesc prelucrarea datelor, informații ce includ: operatorul, datele prelucrate, scopurile în care sunt prelucrate etc.

Pentru mai multe detalii vezi Capitolul III. Cartografierea dateloer personale pe care le procesează organizația.

[11] Art. 30 GDPR.

C. Evaluarea impactului asupra protecției datelor și respectării drepturilor persoanelor fizice[12] (DPIA)

GDPR prevede la art. 35 că operatorul de date este obligat să efectueze o evaluare de impact asupra protecției datelor (sau "**DPIA**") în situațiile susceptibile să genereze **un risc ridicat pentru drepturile și libertățile persoanelor fizice**, enumerând câteva scenarii în care este obligatoriu, fără a fi o lista exhaustivă.

Dintre cele enumerate, relevanta pentru ONG-uri este situația în care are loc o **prelucrare pe scară largă a unor categorii speciale de date.**

Evaluare de impact presupune de fapt **analiza pas cu pas a activității de prelucrare a datelor personale în situațiile care prezintă un risc ridicat și identificarea măsurilor ce trebuie luate pentru a oferi protecția potrivită**. DPIA este implementată cu sprijinul DPO și ajută operatorul să identifice și să stabilească toate riscurile pe care prelucrarea le poate genera.

Această analiză cuprinde:

- descrierea operațiunilor de prelucrare și a scopurilor,
- evaluarea necesității și proporționalității operațiunilor,
- evaluarea riscurilor pentru drepturile și libertățile cetățeanului vizat și măsurile avute în vedere pentru abordarea acestor riscuri.

Pentru mai multe detalii vezi Capitolul IV. Prelucrarea dateloer personale cu caracter special, Secțiunea 2.

5. Implementarea unei politici de prelucrare a datelor la nivelul ONG-ului și elaborarea notelor de informare

Pentru a asigura respectarea obligațiilor impuse de GDPR, ONG-ul **trebuie să ia măsuri concrete pentru punerea lor în practică și să documenteze respectarea lor**.

Aceste măsuri concrete vor fi prevăzute într-o **Politică de prelucrare a datelor personale la nivelul ONG-ului**. De asemenea, ONG-ul trebuie **să aducă la cunoștință această politică de prelucrare a datelor persoanelor ale căror date le colectează**, pentru a asigura corecta informare a persoanelor ale căror date le colectează.

5.1 Politica de prelucrare a datelor personale la nivelul ONG-ului

Ce este Politica de prelucrare a datelor personale?

Politica de prelucrare a datelor personale la nivelul organizației presupune adoptarea

[12] Art. 35 GDPR.

de **măsuri concrete** de respectare a limitărilor colectării și implementarea obligațiilor prevăzute de GDPR

Pentru a putea dovedi respectarea acestor obligații și luarea tuturor măsurilor prevăzute de GDPR, operatorul de date trebuie să dezvolte și să implementeze o **Politică de prelucrare a datelor personale** la nivelul organizației care să traducă în măsuri concrete toate aceste obligații.

Politica de prelucrare a datelor prevede cum folosește organizația datele pe care le colectează și este un instrument care servește reprezentanților și angajaților (inclusiv voluntarii) și colaboratorilor organizației.

Cum se asigură implementarea Politici de prelucrare a datelor personale?

Politica de prelucrare a datelor trebuie comunicată angajaților. **DPO-ul** va fi cel care va asigura o instruire a angajaților cu privire la măsurile pe care ONG-ul le ia pentru a se conforma GDPR.

Cum se construiește o Politică generală de prelucrare a datelor personale?

Politica de prelucrare a datelor personale la nivelul organizației trebuie să aibă în vedere două concepte prevăzute de GDPR: **privacy by design** și **privacy by default**

- **Privacy by design**[13] - presupune luarea în considerare a standardelor de protecție a datelor cu caracter personal încă de la momentul proiectării unei prelucrări și identificarea măsurilor ce trebuie luate: minimizarea colectării datelor în funcție de scop, stabilirea perioadei de stocare, stabilirea informațiilor ce trebuie furnizate persoanelor vizate, obținerea consimțământului persoanelor vizate, stabilirea măsurilor pentru securitatea și confidențialitatea datelor cu caracter personal, garantarea rolului și responsabilității părților implicate în efectuarea prelucrării datelor.

- **Privacy by default**[14] - presupune aplicarea de măsuri tehnice și organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării având în vedere: volumul de date colectate, gradul de prelucrare a acestora, perioada de stocare și accesibilitatea lor, astfel încât datele cu caracter personal să nu fie accesate, de un număr nelimitat de persoane;

  » sensibilizarea și organizarea diseminării informației, în special prin stabilirea unui plan de pregătire și de comunicare cu persoanele care prelucrează date cu caracter personal;

  » soluționarea plângerilor și cererilor adresate de persoanele vizate în exercitarea drepturilor lor, stabilind părțile responsabile de soluționare și modalitățile concrete de exercitare a acestor drepturi; exercitarea drepturilor trebuie să se poată realiza inclusiv pe cale electronică, în cazul în care datele au fost colectate prin astfel de mijloace;

[13] Art. 25 GDPR.

[14] Art. 25 GDPR.

» anticiparea unei posibile încălcări a securității datelor specificând, pentru anumite cazuri, obligativitatea notificării autorității pentru protecția datelor în termen de 72 de ore și a persoanelor vizate în cel mai scurt timp; stabilirea pașilor de urmat în cazul identificării unui incident.

» asigurarea confidențialității și securității prelucrării prin adoptarea de măsuri tehnice și organizatorice adecvate, incluzând printre altele, după caz:

a) pseudonim zarea 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 care sa permită periodic testarea și evaluarea.

CHECKLIST: Ce trebuie să conțină politica de prelucrare a datelor la nivelul organizației[15]

☑ Registrul de evidență a prelucrărilor datelor la nivelul ONG-ului (art. 30 GDPR): măsuri despre cum se completează, cine are atribuții în acest sens, cum se modifică etc.

☑ Prevederi referitoare la pregătirea și instruirea personalului care prelucrează date cu caracter personal

☑ Procedură pentru asigurarea securității prelucrării datelor, cerințe de securitate ce vor fi aplicate pentru activitatea organizației;

☑ Informații despre Responsabilul cu protecția datelor personale la nivelul ONG-ului (cine este, ce atribuții îndeplinește în mod specific)

☑ Modalitate de realizare a proiectelor care implica prelucrarea datelor cu caracter personal (de exemplu, cerințe prind întocmirea planurilor de proiect, notele de informare).

☑ Procedură referitoare la registru de încălcări ale securității datelor unde să fie documentate incidentele (și cele notificate și cele care nu trebuie notificate, împreună cu concluziile analizei incidentului);

☑ Măsurile ce trebuie luate pentru a se asigura detectarea la timp a incidentului de securitate (aplicate pe activitatea organizației efectiv) și notificarea, după caz;

☑ Procedură internă pentru a rezolva solicitările persoanelor vizate;

☑ Condițiile în care se realizează evaluările de impact privind protecția datelor: responsabilități, procedură de aprobare, monitorizare implementare măsuri etc.

☑ Asigurarea obținerii unui consimțământ informat din partea persoanelor vizate, atunci când prelucrarea se bazează pe consimțământ;

☑ Procedură internă cu privire la fluxul de date care să asigure acuratețea și actualizarea datelor;

[15] Lista de mai jos nu este exhaustivă.

☑ Procedură internă de arhivare și ștergere a datelor care nu mai sunt necesare scopului pentru care au fost colectate cu atenție la termenele prevăzute de lege pentru stocarea unor documente supuse unor obligații legale;

☑ Procedură cu privire la evaluarea partenerilor contractuali și la obligația de a adăuga prevederi specifice în cazul în care partenerul contractual acționează ca persoană împuternicită de organizație;

5.2 Note de informare cu privire la prelucrarea datelor personale

Anumite măsuri prevăzute în Politica de prelucrare a datelor personale trebuie comunicate și persoanelor vizate (persoanelor ale căror date le prelucrăm) într-un mod accesibil, de exemplu, **prin publicarea pe site-ul organizației**.

Textele informative cu privire la prelucrarea datelor adresate persoanelor vizate sunt denumite generic **Note de informare** care pot fi generale sau specifice. Scopul lor este asigurarea respectării **principiului transparenței** prevăzut de GDPR.

Nota de informare servește informării persoanelor fizice ale căror date sunt prelucrate cu privire la drepturile lor, scopul pentru care ONG-ul prelucrează datele personale, măsurile de securitate pe care ONG-ul le ia, precum și punerea la dispoziție persoanei vizate unui canal de comunicare cu ONG-ul.

Notele informative generale sunt de exemplu politicile publicate pe site-ul organizației care acoperă informarea cu privire la activitățile de prelucrare desfășurate în general și care este adresată în special persoanelor cu care nu comunică în mod direct și personal (utilizatori website, persoane care adresează solicitări organizației fără să fi avut o legătură anterioară, reprezentanți persoane fizice ale partenerilor persoane juridice etc.).

Sunt numite și: politică de confidențialitate, politica de prelucrare a datelor, notă de informare, informare privind prelucrarea datelor etc.

Cele specifice sunt informările incluse în formulare/proiecte/documente specifice care descriu persoanei vizate ce se întâmplă cu datele furnizate fix în acel context, de exemplu: datele incluse într-un formular de consimțământ pentru a fi fotografiat, pentru a participa la un eveniment, informare pe pagina de proiect cu privire la utilizarea datelor în proiectul respectiv în mod specific etc.

Se recomandă utilizarea ambelor tipuri de note de informare: **o notă informativă generală publicată pe website** care să descrie activitățile desfășurate de organizație cu titlu permanent și **a unei note de informare specifice pentru fiecare proiect**.

Notele de informare (generale și specifice) trebuie să conțină informațiile enumerate la **art. 13 și 14 din GDPR**.

II. Ce ne dă dreptul să prelucrăm date personale

(Temeiuri prevăzute de lege care permit prelucrarea datelor personale)

Atunci când inițiază activități care implică prelucrarea de date cu caracter personal, ONG-ul trebuie întotdeauna să analizeze care este temeiul legal adecvat pentru prelucrarea avută în vedere[1]. Art. 6 din Regulament enumeră temeiurile care ne permit prelucrarea de date personale.

Art. 6 GDPR

(1) Prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:

(a) persoana vizată și-a dat **consimțământul** pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;

(b) prelucrarea este necesară pentru **executarea unui contract** la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;

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

(d) prelucrarea este necesară **pentru a proteja interesele 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 investit operatorul;

(f) prelucrarea este necesară **în scopul intereselor legitime urmărite** de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil. (...)

(3) Temeiul pentru prelucrarea menționată la alineatul (1) literele (c) și (e) trebuie să fie prevăzut în: (a) dreptul Uniunii; sau (b) dreptul intern care se aplică operatorului.

1. Consimțământ

Conform Art. 4 (1) GDPR consimțământ înseamnă „orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate"

[1] Ghidul privind consimțământul, Grupul de lucru „Articolul 29" privind protecția datelor, p. 3 (https://www.dataprotection.ro/servlet/ViewDocument?id=1600).

Consimțământul este un temei legal adecvat doar în cazul în care persoanei vizate **i se oferă controlul și i se dă posibilitatea reală de a face o alegere** în ceea ce privește acceptarea sau refuzarea termenelor oferite sau respingerea acestora fără a fi prejudiciată. Atunci când solicită consimțământul persoanelor fizice ONG-ul trebuie să se asigure că solicitarea îndeplinește toate condițiile pentru obținerea unui consimțământ valabil, așa cum prevede GDPR (de exemplu este esențial ca solicitarea consimțământului să fie precedată de o informare completă).

Consimțământul este un instrument care oferă persoanelor vizate posibilitatea de a controla dacă datele lor cu caracter personal vor fi sau nu prelucrate. În caz contrar, controlul deținut de persoana vizată devine iluzoriu, iar consimțământul nu va constitui un temei valabil pentru prelucrare, făcând ca activitatea de prelucrare să fie ilegală[2].

Obținerea consimțământului nu exclude sau diminuează în vreun fel nici obligațiile operatorului de a respecta principiile de prelucrare. Chiar dacă prelucrarea datelor cu caracter personal se întemeiază pe consimțământul persoanei vizate, acest lucru nu ar justifica colectarea de date care nu este necesară în raport cu un scop specific de prelucrare[3].

1.1 Elementele consimțământului valabil[4]:

A. Liber exprimat

B. Specific

C. Informat

D. Lipsit de ambiguitate

A. Liber exprimat

Persoana vizată trebuie să poată face o alegere reală și să aibă un control real asupra colectării și datelor sale.

Consimțământul **nu va fi considerat liber exprimat** dacă:

- persoana vizată nu este în măsură să refuze sau să-și retragă consimțământul fără a fi prejudiciată
- se simte obligată să consimtă sau va suporta consecințe negative dacă nu consimte

[2] Ghidul privind consimțământul, Grupul de lucru „Articolul 29" privind protecția datelor, p. 3 (https://www.dataprotection.ro/servlet/ViewDocument?id=1600).

[3] Ghidul privind consimțământul, p. 4.

[4] Art. 4 pct. 11 GDPR.

Atenție deosebită trebuie acordată următoarelor situații în care se cere consimțământul persoanei:

Dacă există un dezechilibru de putere în relația dintre ONG și persoana vizată

În relațiile de muncă dintre ONG și angajații săi există un dezechilibru de putere datorită dependenței care rezultă din relația angajat-angajator. Există date cu caracter personal care sunt prelucrate în cadrul relației dintre angajator și angajat necesare încheierii contractului de muncă, fără de care aceasta nu poate fi încheiat (nume, prenume, CNP, cont bancar pentru plata salariului). De cele mai multe ori, aceste date sunt colectate ca urmare a unei obligații impuse de lege, însă nu întotdeauna. ONG-ul trebuie să acorde atenție deosebită datelor pe care le colectează de la angajații săi și să identifice corect temeiul în baza cărora le colectează.

Este discutabil dacă un angajat va răspunde în mod liber la o cerere de consimțământ din partea angajatorului său fără a se teme de consecințe negative în cazul unui refuz[5]. De aceea se recomandă ca datele personale ale angajaților să nu fie prelucrate în temeiul consimțământului întrucât este puțin probabil ca acesta să fie dat în mod liber.

Dacă temeiul va fi consimțământul, ONG-ul trebuie să îl ceară într-un mod în care să fie foarte clar scopul pentru care colectează acele date și mai ales să îi asigure în mod real și concret posibilitatea de a refuza prelucrarea. Consimțământul **este valabil** numai dacă persoana vizată este capabilă să facă o alegere reală și nu există risc de înșelăciune, intimidare, coerciție sau consecințe negative semnificative (de exemplu, costuri suplimentare substanțiale) dacă aceasta nu consimte[6].

Dacă furnizarea unui serviciu sau executarea unui contract este condiționată de acordarea consimțământului

Consimțământul nu va fi considerat liber exprimat în cazul în care executare unui contract sau de furnizarea unui serviciu de **care nu sunt necesare pentru executarea contractului sau serviciului respectiv** este condiționată de acordul pentru cererea de consimțământ pentru prelucrarea datelor cu caracter personal[7].

Consimțământul pentru prelucrarea datelor cu caracter personal care nu sunt necesare **nu poate fi considerat o contraprestație obligatorie** în schimbul executării unui contract sau furnizării unui serviciu[8].

---

[5] De exemplu, în cazul în care se solicită consimțământul pentru a activa sisteme de monitorizare, cum ar fi camerele de supraveghere la locul de muncă, sau pentru a completa formulare de evaluare . Ghidul privind consimțământul, p. 7.

[6] Ghidul privind consimțământul, p. 8.

[7] Considerentul 43 GDPR: "Consimțământul este considerat a nu fi acordat în mod liber în cazul în care aceasta nu permite să se acorde consimțământul separat pentru diferitele operațiuni de prelucrare a datelor cu caracter personal, deși acest lucru este adecvat în cazul particular, sau dacă executarea unui contract, inclusiv furnizarea unui serviciu, este condiționată de consimțământ, în ciuda faptului că consimțământul în cauză nu este necesar pentru executarea contractului"

[8] Ghidul privind consimțământul, p. 9.

Dacă datele personale ale persoanei vizate se prelucrează pentru mai multe scopuri

O activitate desfășurată de ONG poate implica multiple operațiuni de prelucrare a datelor personale **în mai multe scopur**i. Dacă prelucrarea datelor se face în mai multe scopuri, consimțământul ar trebui dat pentru toate scopurile prelucrării în parte.

În astfel de cazuri, persoanele vizate ar trebui să fie libere să aleagă scopul pe care îl acceptă și nu să consimtă la un pachet de scopuri de prelucrare.

De exemplu, în cazul în care ONG-ul dorește să colecteze datele de contact ale participanților la un eveniment pentru a le transmite materialele relevante ulterior încheierii evenimentului, dar și pentru a-i include în baza de date pentru comunicarea despre evenimente viitoare, trebuie să ceară consimțământul pentru fiecare dintre aceste scopuri în parte.

De exemplu, dacă ONG-ul dezvoltă o aplicație care are ca scop furnizarea de informații despre probleme identificate de cetățeni într-un oraș prin încărcarea de fotografii cu problemele rezolvate și nu este necesar pentru funcționarea acesteia să înregistreze/acceseze date de locație sau să acceseze agenda persoanei vizate. Aceste date nu ar trebui colectate pentru că nu sunt necesare scopului principal de prelucrare a informațiilor furnizate de persoana vizată pentru care accesul la galeria de imagini e suficient.

Refuzul sau retragerea consimțământului trebuie să poată fi făcut fără prejudiciu. ONG-ul trebuie să demonstreze că este posibil să se refuze sau să se retragă consimțământul fără prejudiciu[9].

B. Specific

Obținerea unui consimțământ valabil este precedată întotdeauna de stabilirea unui scop specific, explicit și legitim pentru activitatea de prelucrare preconizată[10].

ONG-ul care solicită consimțământul **pentru o serie de scopuri diferite** ar trebui să ofere o opțiune separată pentru fiecare scop în parte, astfel încât să permită utilizatorilor să acorde **un consimțământ specific pentru scopuri specifice**.

Consimțământul poate viza diferite operațiuni, atât timp cât respectivele operațiuni servesc aceluiași scop.

ONG-ul trebuie să furnizeze informații specifice, împreună cu fiecare cerere separată de consimțământ, referitoare la datele care sunt prelucrate în fiecare scop, pentru ca persoanele vizate să fie conștiente de impactul diferitelor opțiuni pe care le au la dispoziție. Astfel, persoanele vizate au posibilitatea de a exprima un consimțământ specific.

[9] Considerentul 42, GDPR.

[10] Art. 5 alin. (1) litera (b) GDPR.

C. Informat

Furnizarea de informații persoanelor vizate înainte de obținerea consimțământului acestora este esențială pentru a le permite să ia decizii în cunoștință de cauză, să înțeleagă aspectele față de care își exprimă acordul și, de exemplu, să își exercite dreptul de a-și retrage consimțământul. Dacă operatorul nu furnizează informații accesibile, controlul utilizatorului devine iluzoriu, iar consimțământul nu va constitui un temei valabil pentru prelucrare[11].

Este necesar ca persoana vizată să fie informată cu privire la anumite elemente care sunt esențiale pentru a face o alegere. **Informarea va include cel puțin următoarele informații:**

- identitatea operatorului,
- scopul fiecărei operațiuni de prelucrare pentru care se solicită consimțământul,
- tipul de date care vor fi colectate și utilizate,
- existența dreptului de retragere a consimțământului

În funcție de caz, pot fi necesare mai multe informații pentru a permite persoanei vizate să înțeleagă cu adevărat ce operațiuni de prelucrare sunt în discuție.

Cererea de solicitare a consimțământului trebuie să folosească un limbaj adecvat persoanelor ale căror date urmează să le prelucreze. În cazul ONG-urilor limbajul trebuie să fie clar și simplu astfel încât să fie ușor de înțeles pentru o persoana obișnuită care nu are pregătire în domeniul GDPR. Folosirea unor politici de confidențialitate lungi care conțin limbaj tehnic și care sunt dificil de înțeles nu vor satisface condiția unui consimțământ informat.

Consimțământul trebuie să fie clar, să poată fi deosebit de alte aspecte și să fie furnizat într-o formă inteligibilă și ușor accesibilă.

De asemenea, în cazul în care consimțământul este solicitat prin mijloace electronice, cererea de consimțământ trebuie să fie separată și distinctă, neputând fi doar un alineat din cadrul termenelor și condițiilor[12].

D. Lipsit de ambiguitate

Trebuie să fie evident că persoana vizată a acordat consimțământul pentru o anumită prelucrare.

Acțiunea prin care este acordat consimțământul trebuie să se poată deosebi de alte acțiuni. Tăcerea sau inactivitatea persoanei vizate, precum și simpla continuare a unui serviciu nu pot fi considerate drept manifestări active ale alegerii.

---

[11] Ghidul privind consimțământul, p. 14.

[12] Considerentul 32, GDPR.

În contextul mediului online, utilizarea opțiunilor implicite pe care persoana vizată trebuie să le modifice pentru a respinge prelucrarea („consimțământul bazat pe tăcere") nu constituie, în sine, un consimțământ valabil.

1.2 Durata de valabilitate a consimțământului

Durata de valabilitate a consimțământului va depinde de context, de domeniul de aplicare a consimțământului inițial și de așteptările persoanei vizate. De aceea este foarte important ca înainte de prelucrare să fie identificat scopul specific al prelucrării.

Se recomandă actualizarea consimțământului la intervale adecvate. Este de asemenea important ca durata de valabilitate a consimțământului să fie corelată scopului specific al prelucrării.

De exemplu, în cazul în care ONG-ul are o bază de date are conține datele de contact ale persoanelor care și-au exprimat acordul pentru a le fi comunicat regulat informații despre activitatea ONG-ului. Acest consimțământ nu poate fi dat pe perioadă nedeterminată și ar trebui actualizat la un interval adecvat, stabilit de către ONG.

În cazul în care consimțământul pentru prelucrarea unor date se cere pentru desfășurarea unei activități cu perioadă determinată, atunci consimțământul acordat va fi valabil pe durata desfășurării activității sau până la retragerea expresă a acestuia de către persoana vizată.

1.3 Nota de informare

Acordarea consimțământului este în mod obligatoriu precedat de **Nota de informare** cu privire la colectarea datelor. Această Notă de informare trebuie comunicată persoanei vizate de către ONG. Nota de informare poate fi inclusă în formularul care se completează de persoana vizată pentru acordarea consimțământului.

Nota de informare trebuie să includă obligatoriu:

A. Datele de identificare a ONG-ului care colectează datele

B. Ce date colectează ONG-ul

C. Cu ce scop

D. Temeiul colectării

E. Pe ce durată are loc colectarea și stocarea datelor

F. Drepturile persoanei vizate cu privire la datele colectate, în mod deosebit informații despre modalitatea de retragere a consimțământului

1.4 Demonstrarea consimțământului

Consimțământul trebuie să vizeze toate activitățile de prelucrare efectuate în același scop sau în aceleași scopuri. Dacă prelucrarea datelor se face în mai multe scopuri, consimțământul trebuie dat pentru toate scopurile prelucrării.

Operatorul trebuie să demonstreze obținerea consimțământului persoanei vizate și în acest sens trebuie să documenteze întreg procesul de obținere a acestuia[13].

ONG-ul trebuie **să țină o evidență a declarațiilor de consimțământ primite** (online/offline, în funcție de caz), astfel încât să poată arăta că au fost îndeplinite condițiile necesar acordării unui consimțământ valid:

- modul în care a fost obținut consimțământul,
- momentul când a fost obținut consimțământul
- informațiile furnizate persoanei vizate în vederea solicitării consimțământului.

De exemplu, într-un context online, un operator ar putea să păstreze informații despre sesiunea în care a fost exprimat consimțământul, împreună cu documentația fluxului de lucru privind consimțământul la momentul sesiunii, precum și o copie a informațiilor care au fost prezentate persoanei vizate la acel moment[14].

Cum se poate documenta acordarea consimțământului:

- **declarație făcută în scris** într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu; trebuie să vă asigurați că persoana vizată este informată cu privire la datele care îi sunt colectate, scopul prelucrării și drepturile pe care le are cu privire la aceste date
- **declarație în format electronic** precum bifarea unei căsuțe atunci când persoana vizitează un site; însă, **atenție**, utilizarea căsuțelor de participare **pre-bifate** nu este validă în temeiul GDPR.
- **declarație exprimată verbal, ideal înregistrată**, deși trebuie să se țină seama în mod corespunzător de informațiile puse la dispoziția persoanei vizate înainte de manifestarea consimțământului

1.5 Retragerea consimțământului

Colectarea datelor personale în baza consimțământului înseamnă că persoana vizată are control deplin asupra datelor sale și poate dispune în orice moment de ele. ONG-ul trebuie să informeze persoana vizată asupra dreptului de retragere a consimțământului înainte de acordarea efectivă a consimțământului[15].

Atenție: Atunci când ONG-ul nu va putea să șteargă datele persoanei în cazul în care aceasta își retrage consimțământul pentru că, de exemplu, are nevoie de ele ca să le raporteze unei autorități (de exemplu, ANAF) sau ștergerea datelor imposibilă prestarea unui serviciu, înseamnă că temeiul meu de prelucrare nu a fost corect identificat ca fiind consimțământul persoanei.

[13] Art. 7 alin. (1) GDPR.

[14] Ghidul privind consimțământul, p. 23.

[15] Art. 7 alin. (3) GDPR.

În cazul retragerii consimțământului, ca regulă generală, toate operațiunile de prelucrare a datelor care s-au bazat pe consimțământul respectiv și au avut loc înainte de retragerea acestuia continuă să fie legale, însă operatorul trebuie să oprească acțiunile de prelucrare în cauză. Dacă nu există un alt temei legal care să justifice prelucrarea, acestea ar trebui să fie șterse de către operator[16].

De asemenea, nu este permisă utilizarea retroactivă a temeiului privitor la interesul legitim pentru a justifica prelucrarea în cazul în care s-au întâmpinat probleme în legătură cu validitatea consimțământului[17].

Retragerea consimțământului persoanei vizate trebuie să se realizeze cu respectarea **anumitor condiții**, cum ar fi:

- Consimțământul să poată fi retras cu același grad de ușurință cu care a fost acordat și în orice moment
- Consimțământul să poată fi retras fără a fi prejudiciată persoana vizată

Persoanei vizate trebuie să i se comunice care este modalitatea concretă de retragere a consimțământului (de exemplu: datele de contact ale persoanei responsabile de gestionarea datelor și care poate da curs solicitării, link pentru dezabonare etc). Aceste informații trebuie să se regăsească în **Nota de informare.**

2. Contract

Prelucrarea datelor personale este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract.

Atunci când prelucrarea are ca temei un contract, acesta include și fazele premergătoare încheierii contractului.

Precizare importantă: Temeiul de executare a contractului poate fi utilizat doar atunci când ONG-ul are un contract direct cu persoana fizică, nu când persoana fizică semnează ca reprezentant al unei persoane juridice. În acest din urmă caz, temeiul prelucrării datelor reprezentanților/persoanelor de contact va fi interesul legitim al organizației (care poate fi economic sau de altă natură și care derivă din contractul încheiat cu persoana juridică pe care persoana fizică o reprezintă).

Sintagma „**necesar pentru executarea unui contract**" trebuie să fie interpretată strict. Prelucrarea trebuie să fie necesară pentru a executa contractul față de fiecare persoană vizată în mod individual[18].

[16] Ghidul privind consimțământul, p. 25.

[17] Ghidul privind consimțământul, p. 26

[18] Conform Avizului 06/2014 al GL 29.

Trebuie să existe o legătură directă și obiectivă între prelucrarea datelor și scopul executării contractului: de exemplu, prelucrarea detaliilor contului bancar, astfel încât să poată fi plătite salariile.

Atenție: datele personale prelucrate să fie necesare pentru executarea unui contract și să nu existe o situație de înglobare a consimțământului în contract sau de condiționare. Pentru a evalua dacă există o astfel de situație de înglobare a consimțământului sau de condiționare, este important să se determine domeniul de aplicare a contractului și datele care ar fi necesare pentru executarea contractului respectiv.

3. Obligație legală

Atunci când prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine ONG-ului, nu mai este necesară obținerea consimțământului persoanelor vizate (de exemplu, prelucrarea datelor angajaților de către angajator în vederea transmiterii acestora către REVISAL). **Informarea se va face în orice caz, indiferent de temeiul de prelucrare.**

Obligația legală în baza căreia colectăm datele trebuie să fie cât de cât explicită. Prevederile legale foarte rar vor include aspecte legate de prelucrarea datelor personale (ce date trebuie colectate și cum trebuie folosite). Însă dacă prevederea legală obligă la verificarea identității, de exemplu, din care reiese că anumite date trebuie colectate și utilizate pentru a îndeplini obligația legală.

Cel mai frecvent exemplu îl reprezintă situațiile contabile care conțin date de identificare – obligatorii conform prevederilor contabile.

Dacă există o obligație legală sau un contract cu persoana vizată care impun utilizarea anumitor date, atunci acestea se vor impune ca temei și abia în subsidiar vor fi folosite drept temei „consimțământul" sau „interesul legitim". Dacă persoana vizata poate fi contactată și dacă ea are control deplin asupra datelor (poate să își dea sau nu acordul, poate solicita și obține ștergerea datelor în orice moment) atunci se va opta pentru consimțământ. Dacă dimpotrivă, persoana vizată nu poate fi contactata, iar datele sunt utilizate pentru scopuri proprii care nu aduc un beneficiu direct persoanei vizate (cum ar fi dezvoltarea infrastructurii, realizarea de sondaje pentru îmbunătățire, realizarea de rapoarte și alte studii etc.) atunci temeiul ONG-ului va fi interesul legitim.

4. Interes legitim

Art. 9 din Legea nr. 190/2018:

(1) În vederea asigurării proporționalității și a unui echilibru între dreptul la protecția datelor cu caracter personal și a datelor speciale și prelucrarea unor astfel de date de către partidele politice și organizațiile cetățenilor aparținând minorităților naționale, **organizațiilor neguvernamentale**, se vor realiza următoarele garanții:

a) informarea persoanei vizate despre prelucrarea datelor cu caracter personal;

b) garantarea transparenței informațiilor, a comunicărilor și a modalităților de exercitare a drepturilor persoanei vizate;

c) garantarea dreptului de rectificare și ștergere.

(2) Prelucrarea datelor cu caracter personal și special este permisă partidelor politice și organizațiilor cetățenilor aparținând minorităților naționale, organizațiilor neguvernamentale, **în vederea realizării obiectivelor acestora, fără consimțământul expres al persoanei vizate**, dar cu condiția să se prevadă garanțiile corespunzătoare, menționate la alineatul precedent.

Legea 190/2018 prevede că ONG-urile pot să colecteze date personale (inclusiv și cele cu caracter special) **fără a mai cere consimțământul** în baza interesului legitim în vederea realizării obiectivelor acestora în baza interesului legitim al ONG-ului, prevăzând câteva garanții, expres prevăzute de lege:

- Să informeze persoanele vizate despre prelucrarea datelor cu caracter personal. Cu alte cuvinte să elaboreze Note de informare în concordanță cu rigorile impuse de GDPR.
- Să garanteze transparența informațiilor, a comunicărilor și a modalităților de exercitare a drepturilor persoanei vizate
- Să garanteze dreptul de rectificare și ștergere

Însă atunci când prelucrarea se invocă interesul legitim al operatorului, trebuie să fie temeinic justificat și întotdeauna trebuie desfășurată o analiză a interesului legitim care să se regăsească într-o documentație păstrată de organizație (legitimate interest assessment[19] - "LIA") anterior desfășurării activității de prelucrare. Cum nu este sigur că interpretarea conceptului de "interes legitim" va fi aceeași și pentru ONG și pentru Autoritatea de Supraveghere, și cum se va raporta această interpretare la obiectivele organizației, este recomandabil să se obțină consimțământul pentru prelucrare ori de cate ori e posibil și să se asigure toate garanțiile necesare.

[19] Mai multe informații despre cum se face o analiză a interesului legitim găsiți aici: „How do we apply legitimate interests in practice?" (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/).

III. Cartografierea[1] datelor personale pe care le procesează organizația

1. Când este obligatorie cartografiere datelor personale?

Cartografierea este obligatorie[2]:

- în cazul întreprinderilor sau organizațiilor cu mai mult de 250 de angajați;
- atunci când prelucrarea este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate și nu este o prelucrare ocazională;
- prelucrarea include categorii speciale de date (art. 9 GDPR);
- prelucrarea include categorii de date cu caracter personal referitoare la condamnări penale și infracțiuni (art. 10 GDPR).

Însă **este recomandat** ca toți operatorii de date personale să facă și să țină o evidență a prelucrării de date personale la nivelul organizației.

2. Ce presupune cartografierea?

O evidență la nivelul organizației în care identificăm datele personale pe care le colectează organizația răspunzând la următoarele întrebări[3]:

Cine?	Se înscriu în evidența numele și coordonatele operatorului (și ale reprezentantului sau legal) și, după caz, ale responsabilului cu protecția datelor; Se întocmește lista persoanelor împuternicite, după caz.
Ce?	Se identifică categoriile de date cu caracter personal prelucrate; Se identifică datele susceptibile de a prezenta riscuri datorită naturii lor sensibile deosebite
De ce?	Se precizează scopul sau scopurile în care sunt colectate sau prelucrate datele cu caracter personal (de exemplu: gestionarea relației comerciale, managementul resurselor umane, geo-localizare, video-supraveghere etc.
Cum?	Se precizează măsurile de securitate implementate pentru a reduce la minimum riscurile de a acces neautorizat la date și, în consecința, impactul asupra vieții private a persoanelor vizate.
Unde?	Se stabilește locul sistemului de evidentă și, dacă e cazul, destinatarii datelor. Categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe. Se stabilesc statele către care sunt, eventual, transferate datele.
Până când?	Se stabilește locul sistemului de evidentă și, dacă e cazul, destinatarii datelor. Categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe. Se stabilesc statele către care sunt, eventual, transferate datele.

[1] Este folosit și termenul de "mapare" a datelor personale colectate. GDPR folosește termenul de "evidență a activităților de prelucrare"

[2] Art. 30 alin. (5) GDPR.

[3] Art. 30 alin. (1) GDPR.

IV. Prelucrarea datelor personale cu caracter special

Prelucrarea de date cu caracter special așa cum sunt ele definite de GDPR impune operatorului de date să ia măsuri speciale de protecție.

1. Care sunt datele cu caracter special?

Art. 9 din GDPR

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

2. Prelucrarea acestor categorii de date **este permisă numai în următoarele condiții:**

- persoana vizată **și-a dat consimțământul explicit** pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice;
- prelucrarea 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;
- prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul;
- prelucrarea este efectuată în cadrul activităților lor legitime și cu garanții adecvate de către o fundație, o asociație sau orice alt organism fără scop lucrativ și cu specific politic, filozofic, religios sau sindical;
- prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;
- prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare;
- prelucrarea este necesară din motive de interes public major, în baza dreptului UE sau a dreptului intern;
- 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 sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială;

- 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 sau a dispozitivelor medicale;
- prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice.
- prelucrarea datelor genetice, biometrice sau a datelor privind sănătatea, în scopul realizării unui proces decizional automatizat sau pentru crearea de profiluri, este permisă cu consimțământul explicit al persoanei vizate sau dacă prelucrarea este efectuată în temeiul unor dispoziții legale exprese, cu instituirea unor măsuri corespunzătoare pentru protejarea drepturilor, libertăților şi intereselor legitime ale persoanei vizate.

2. Care sunt măsurile speciale care se impun când sunt prelucrate date personale cu caracter special?

Dacă ONG-ul poate identifica un temei pentru prelucrarea datelor cu caracter special dintre cele enumerate mai sus[1], atunci trebuie să se asigure că în cadrul organizației numește un **Responsabil cu protecția datelor personale (DPO)**. Cu sprijinul DPO se efectuează o **evaluare de impact (DPIA)** înainte de începerea prelucrării, și se verifică documentarea strictă a măsurilor luate pentru ca apoi să se poată face dovada implementării lor.

2.1 Numirea unui Responsabil cu protecția datelor personale (DPO)

A. Când este obligatoriu DPO-ul?

Este obligatoriu ca ONG-ul să numească un DPO dacă[2]:

1. Prelucrează date cu caracter special pe scară largă sau date cu caracter personal privind condamnări penale și infracțiuni
2. Activitățile principale ale ONG-ului constau în operațiuni de prelucrare care, prin natura, domeniul de aplicare și/sau scopurile lor, necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă
3. Prelucrarea este efectuată de o autoritate sau un organism public (în cazul ONG-urilor o asociație sau fundație de utilitate publică)

Chiar și atunci când nu există obligația legală de a numi un DPO, este recomandat ca ONG-ul să aibă o persoană responsabilă cu protecția datelor personale care să asigure instruirea angajaților cu privire la standardele GDPR, să elaboreze politica interna a ONG-ului cu privire la prelucrarea acestor date și să ofere îndrumare atunci când ONG-ul colectează date personale cu caracter special.

[1] Așa cum sunt prevăzute la art. 9. alin. (2) GDPR.

[2] Art. 37 GDPR, corelat cu art. 10 din Legea 190/2018.

B. Rolul DPO-ului[3]:

(a) să informeze și să consilieze operatorul sau persoana împuternicită de operator, precum și angajații care se ocupă de prelucrare cu privire la obligațiile care le revin în domeniul protecției datelor cu caracter personal

(b) să monitorizeze respectarea GDPR și a altor prevederi legale în domeniul protecției datelor personale și a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce privește GDPR, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;

(c) să furnizeze consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia

(d) să coopereze cu autoritatea de supraveghere și să își asume rolul de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare

C. Ce condiții trebuie să îndeplinească DPO-ul

DPO-ul poate fi un desemnat dintre membrii/angajații ONG-ului sau poate fi o persoană care îndeplinește această sarcină în baza unui contract de prestări de servicii. De asemenea, o persoană poate îndeplini rolul de DPO pentru mai multe organizații.

Este recomandat ca, în măsura în care ONG-ul nu are resursele pentru a externaliza această funcție către o persoană cu cunoștințe de specialitate cu privire la protecția datelor personale, să fie desemnată ca DPO persoana din cadrul ONG-ului care are capacitatea de a se familiariza cu prevederile legale în domeniu.

Atentie! **Nu poate fi DPO o persoană care are putere de decizie la nivelul ONG-ului** (membru în consiliul director, președinte, director executiv etc.), pentru a se evita conflictele de interese.

DPO-ului trebuie să i se asigure resursele necesare pentru executarea acestor sarcini pentru menținerea cunoștințelor sale de specialitate, precum și accesul la datele cu caracter personal și a operațiunilor de prelucrare.

Operatorul și persoana împuternicită de operator se asigură că responsabilul cu protecția datelor **DPO-ul beneficiază de independență** în îndeplinirea acestor sarcini și ONG-ul (și persoanele împuternicite de ONG) trebuie să se asigure că nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea acestor sarcini.

DPO-ul **răspunde direct în fața celui mai înalt nivel al conducerii** ONG-ului sau persoanei împuternicite de acesta.

DPO-ul nu poate fi demis sau sancționat de către ONG sau de persoana împuternicită de operator pentru îndeplinirea sarcinilor sale.

DPO-ul are **obligația de a respecta secretul sau confidențialitatea** în ceea ce privește îndeplinirea sarcinilor sale.

[3] Art. 39 GDPR.

2.2 Efectuarea unei evaluări de impact ("data protection impact assessment" – "DPIA")

A. Ce este DPIA?

DPIA constă în efectuarea, înaintea prelucrării, a unei analize a operațiunilor de prelucrare de date personale la nivelul ONG-ului atunci când prelucrarea preconizată poate să genereze **un risc ridicat pentru drepturile și libertățile persoanei vizate**.

DPIA este un proces de consolidare și demonstrare a conformității[4].

B. Când este necesară?

GDPR nu prevede efectuarea unei DPIA pentru fiecare operațiune de prelucrare care poate genera riscuri pentru drepturile și libertățile persoanelor fizice ale căror date le prelucrează. O DPIA este necesară **numai atunci** când prelucrarea este „susceptibilă să genereze **un risc ridicat pentru drepturile și libertățile persoanelor fizice"**[5].

DPIA este necesară **în special în următoarele situații**[6]:

1. prelucrarea datelor cu caracter personal efectuată în vederea **realizării unei evaluări sistematice** şi cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, şi care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

2. **prelucrarea pe scară largă a datelor cu caracter personal sensibile** privind originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate, a datelor genetice, a datelor biometrice pentru identificarea unică a unei persoane fizice, a datelor privind sănătatea, viața sexuală sau orientarea sexuală ale unei persoane fizice sau a datelor cu caracter personal referitoare la condamnări penale şi infracțiuni;

3. **prelucrarea datelor cu caracter personal având ca scop monitorizarea sistematică pe scară largă a unei zone accesibile publicului**, cum ar fi supravegherea video în centre comerciale, stadioane, piețe, parcuri sau alte asemenea spații;

4. **prelucrarea pe scară largă a datelor cu caracter personal ale persoanelor vulnerabile**, în special ale minorilor şi ale angajaților, prin mijloace automate de monitorizare şi/sau înregistrare sistematică a comportamentului, inclusiv în vederea desfăşurării activităților de reclamă, marketing şi publicitate;

5. **prelucrarea pe scară largă a datelor cu caracter personal prin utilizarea inovatoare sau implementarea unor tehnologii noi**, în special în cazul în care

---

[4] Ghidul privind evaluarea impactului asupra protecției datelor (DPIA), Grupul de lucru pentru protecția datelor instituit în temeiul art. 29, p. 4 (https://www.dataprotection.ro/?page=Comunicat_ghid_final_DPIA&lang=ro)

[5] Art. 35 alin. 1 GDPR

[6] Decizia președintelui autorității de supraveghere nr. 174/2018 privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal (https://www.dataprotection.ro/servlet/ViewDocument?id=1556)

operațiunile respective limitează capacitatea persoanelor vizate de a-şi exercita drepturile, cum ar fi utilizarea tehnicilor de recunoaştere facială în vederea facilitării accesului în diferite spații;

6. **prelucrarea pe scară largă a datelor generate de dispozitive cu senzori care transmit date prin internet sau prin alte mijloace** (aplicații "Internetul lucrurilor", cum ar fi smart TV, vehicule conectate, contoare inteligente, jucării inteligente, oraşe inteligente sau alte asemenea aplicații);

7. **prelucrarea pe scară largă şi/sau sistematică a datelor de trafic şi/sau de localizare a persoanelor fizice** (cum ar fi monitorizarea prin Wi-Fi, prelucrarea datelor de localizare geografică a pasagerilor în transportul public sau alte asemenea situații) atunci când prelucrarea nu este necesară pentru prestarea unui serviciu solicitat de persoana vizată.

În cazurile în care **nu este clar dacă este necesară o DPIA**, se recomandă efectuarea acesteia, întrucât o DPIA este un instrument util care sprijină organizația în respectarea legislației în materie de protecție a datelor[7].

Ce înseamnă "prelucrare la scară largă"?

GDPR nu definește conceptul de **"pe scară largă"**. Se recomandă[8] ca în special următorii factori să fie luați în considerare atunci când se stabilește dacă prelucrarea se efectuează pe scară largă:

- numărul de persoane vizate în cauză, fie ca număr specific sau ca proporție din populația relevantă;
- volumul de date și/sau gama de diferite elemente de date care sunt prelucrate;
- durata sau persistența activității de prelucrare a datelor;
- extinderea geografică a activității de prelucrare.

Ce înseamnă “persoane vulnerabile”[9] din perspectiva GDPR?

Prelucrarea acestui tip de date reprezintă un criteriu din cauza dezechilibrului de putere crescut dintre persoanele vizate și operatorul de date. Acest dezechilibru înseamnă că persoanele pot să nu fie în măsură să își dea consimțământul în mod liber sau să respingă cu ușurință prelucrarea datelor lor sau să își exercite drepturile.

Această categorie poate include copii (aceștia pot fi considerați ca nefiind în măsură să se opună sau să își dea consimțământul în mod deliberat și precaut pentru prelucrarea datelor lor), angajați, segmente mai vulnerabile ale populației care necesită o protecție specială (persoane bolnave mintal, solicitanții de azil sau persoanele în vârstă, pacienți etc.) și, în orice caz, atunci când poate fi identificat un dezechilibru între poziția persoanei vizate și cea a operatorului.

---

[7] Ghidul privind evaluarea impactului asupra protecției datelor (DPIA), p. 8.

[8] Ghidul privind evaluarea impactului asupra protecției datelor (DPIA), p. 10.

[9] GDPR, considerentul 75.

C. În ce constă DPIA

Elementele minime ale unei DPIA sunt[10]:

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

DPIA este **un instrument de gestionare a riscurilor pentru drepturile persoanelor vizate** și, prin urmare, se axează pe măsurile care vor fi luate pentru reducerea riscurilor din perspectiva persoanelor fizice vizate, nu cea a organizației. Operatorul de date are libertatea să decidă structura și forma exactă a DPIA pentru a permite ca aceasta să fie adaptata practicilor de lucru existente[11].

În DPIA trebuie să se stabilească partea responsabilă pentru diferitele măsuri destinate să trateze riscurile și să protejeze drepturile și libertățile persoanelor vizate..

O DPIA poate să vizeze o singură operațiune de prelucrare a datelor, dar este posibil ca o DPIA să abordeze un set de operațiuni de prelucrare similare în ceea ce privește natura, domeniul de aplicare, contextul, scopul și riscurile[12].

Exemplu de prelucrare care necesită o DPIA[13]: *O organizație care monitorizează sistematic activitățile angajaților săi, inclusiv monitorizarea stațiilor de lucru, a activității pe internet a angajaților săi etc. - monitorizare sistematică și date referitoare la persoanele vizate vulnerabile*

Exemplu de prelucrare care nu necesită o DPIA[14]: *O revistă online care folosește o listă de corespondență pentru a trimite un abonament generic zilnic abonaților săi - date prelucrate pe scară largă*

[10] Art. 35 alin. (7) GDPR.

[11] Ghidul privind evaluarea impactului asupra protecției datelor (DPIA), p. 18.

[12] Art. 35 alin. (1) GDPR.

[13] Ghidul privind evaluarea impactului asupra protecției datelor (DPIA), p. 12.

[14] Ghidul privind evaluarea impactului asupra protecției datelor (DPIA), p. 12.

D. Când trebuie făcută DPIA?

DPIA ar trebui să fie elaborată și implementată cât mai curând posibil în elaborarea operațiunii de prelucrare, chiar dacă o parte din operațiunile de prelucrare încă nu sunt cunoscute[15]. Se recomandă ca DPIA să fie revizuită în mod continuu și reevaluată în mod periodic.

E. Consultarea Autorității de Supraveghere

Atunci când DPIA indică faptul **că prelucrarea ar genera un risc ridicat** în absența unor măsuri luate de operator pentru atenuarea riscului, operatorul consultă autoritatea de supraveghere înainte de prelucrare, furnizându-i o serie de informații relevante despre prelucrare, prevăzute la art. 36 GDPR.

[15] Ghidul privind evaluarea impactului asupra protecției datelor (DPIA), p. 15. (https://www.dataprotection.ro/?page=Comunicat_ghid_final_DPIA&lang=ro)

V. Drepturile persoanelor ale căror date sunt prelucreate

Toate aceste informații se vor regăsi în **Nota de informare** a persoanei vizate. Pentru mai multe detalii despre Nota de informare, a se vedea secțiunea 5, Capitolul I. Ce este GDPR și ce obligații generale impune.

În această secțiune detaliem care sunt drepturile persoanelor vizate în raport cu datele personale colectate și cum se exercită ele, din perspectiva GDPR:

1. Drepturile persoanelor vizate Cap. III din GDPR[1]

Dreptul la informare[2]

Persoanele ale căror date sunt prelucrate trebuie să fie informate în mod corect și complet despre prelucrare. Regulamentul stabilește obligația operatorului de date de a asigura un anumit nivel de transparență față de persoana vizată. Acestea trebuie să fie informate cu privire la identitatea operatorului de date, scopul în care le vor fi prelucrate datele, ce date sunt prelucrate, ce drepturi le sunt garantate, cum își pot exercita aceste drepturi și cine sunt terții cărora operatorul le va dezvălui datele, dacă este cazul.

Dreptul de acces la date[3]

Persoana vizată are dreptul de a obține din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc. În cazul în care răspunsul operatorului este afirmativ, persoana vizată are dreptul de a cunoaște și de a i se comunica informații despre datele personale pe care operatorul le deține.

Dreptul la rectificare[4]

În cazul în care datele cu caracter personal sunt inexacte, persoana vizată are dreptul de cere a rectificarea datelor, de către operator, fără întârzieri nejustificate. Aceeași procedură se aplică dacă datele sunt incomplete.

Dreptul la restricționarea prelucrării datelor[5] și **Dreptul la ștergere a datelor**[6] sau "dreptul de a fi uitat". În baza lui personale fizice pot cere ștergerea datelor personale dacă acestea au fost prelucrate ilegal, fără consimțământul acestora sau dacă datele nu mai sunt

---

[1] Pentru mai multe detalii despre drepturile persoanelor vizate și cum se exercită, a se vedea Capitolul V. Drepturile persoanelor ale căror date sunt prelucrate

[2] Art. 13-14 GDPR.

[3] Art. 15 GDPR.

[4] Art. 16 și 19 GDPR.

[5] Art. 18 și 19 GDPR.

[6] Art. 17 și 19 GDPR.

necesare scopului pentru care au fost prelucrate inițial.

Dreptul de a fi uitat nu este unul absolut, fiind necesară o analiză a circumstanțelor specifice fiecărui caz în parte. GDPR permite păstrarea în continuare a datelor cu caracter personal în cazul în care aceasta este necesară pentru respectarea libertății de exprimare și a dreptului la informare, pentru respectarea unei obligații legale, pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice 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 sau pentru constatarea, exercitarea sau apărarea unui drept în instanță[7].

Dreptul la portabilitatea datelor[8]

Oferă posibilitatea persoanei vizate de a cere să se transmită datele sale la un alt operator sau de a primi datele personale care o privesc și pe care le-a furnizat operatorului. Se aplică în cazul în care datele au fost prelucrate în baza consimțământului sau în executarea unui contract. Datele transferate trebuie să fie furnizate într-un format structurat, prelucrabil automat și interoperabil ca să poată fi ușor prelucrate de un alt operator.

Dreptul la opoziție[9]

Persoanele vizate au dreptul de a se opune prelucrării oricăror date cu caracter personal care le privesc, din motive legate de situația particulară în care se află, atunci când datele sunt prelucrate pentru:

- îndeplinirea unei sarcini care servește unui interes public
- îndeplinirea unei sarcini care rezultă din exercitarea autorității publice cu
- care este învestit operatorul
- scopul intereselor legitime ale unui operator sau ale unei părți terțe.
- scopuri de cercetare ştiințifică sau istorică ori în scopuri statistice, cu
- excepția cazului în care prelucrarea este necesară pentru îndeplinirea unei
- sarcini din motive de interes public.

Operatorul trebuie să oprească prelucrarea datelor cu caracter personal, cu excepția cazului în care demonstrează că are motive legitime şi imperioase care justifică prelucrarea şi care prevalează asupra intereselor, drepturilor şi libertăților persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanță.

Dreptul de a nu face obiectul unei decizii automate, profilare[10]

Persoana vizată are dreptul 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.

---

[7] Noul Regulament privind Protecția Datelor – Elemente de noutate, 2018, ANSPDCP

[8] Art. 20 GDPR.

[9] Art. 21 GDPR.

[10] Art. 22 GDPR.

2. Condiții de exercitare a drepturilor

Pentru exercitarea acestor drepturi, persoanele vizate trebuie să adreseze o cerere în acest sens ONG-ului care prelucrează datele. Există condiții specifice de exercitare pentru fiecare dintre aceste drepturi[11].

Operatorul furnizează persoanei vizate informații privind acțiunile întreprinse în urma unei cereri[12] în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu două luni atunci când este necesar, ținându-se seama de complexitatea şi numărul cererilor.

Operatorul informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând şi motivele întârzierii[13].

3. Excepții prevăzute de Legea 190/2018

Prelucrarea de date în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare[14]

Persoana vizată nu își va putea exercita aceste drepturi când prelucrarea datelor personale se face **în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare**, dacă prelucrarea priveşte date cu caracter personal care au fost făcute publice în mod manifest de către persoana vizată sau care sunt strâns legate de calitatea de persoană publică a persoanei vizate ori de caracterul public al faptelor în care este implicată

Prelucrarea de date în scopuri de cercetare ştiințifică sau istorică sau în scopuri statistice ori în scopuri de arhivare în interes public[15]

Dreptul de acces, dreptul la rectificarea datelor, dreptul la restricționarea prelucrării şi dreptul la opoziție din GDPR nu se aplică în cazul în care datele cu caracter personal sunt prelucrate în în scopuri de cercetare ştiințifică sau istorică sau în scopuri statistice ori în scopuri de arhivare în interes public

Aceste derogări se aplică în măsura în care drepturile menționate la aceste articole sunt de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice și sub rezerva existenței garanțiilor corespunzătoare pentru drepturile şi libertățile persoanelor vizate.

---

[11] Pentru mai multe detalii despre cum se exercită aceste drepturi, a se vedea GHID ÎNTREBĂRI ȘI RĂSPUNSURI CU PRIVIRE LA APLICAREA REGULAMENTULUI (UE) 2016/679, ANSPDCP (www.dataprotection.ro)

[12] În temeiul articolelor 15-22 din GDPR.

[13] Art. 12 din GDPR.

[14] Art. 7-8 din Legea 190/2018.

[15] Art. 7-8 din Legea 190/2018

VI. Incidentul de securitate[1]

1. Ce este un incident de securitate?

Incidentul de securitate înseamnă o încălcare a securității datelor care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea. Cele mai multe incidente de securitate sunt cauzate de eroare umană.

De exemplu: e-mailuri trimise greșit (către alți destinatari), documente care ajung în posesia altor persoane decât cele autorizate, lăsate pe birou, ecran întors sau vizibil spre persoane neautorizate, pierderea laptopului pe care se află datele persoanelor, phishing, furnizarea datelor persoanelor către alte persoane neautorizate, probleme tehnice care determină imposibilitatea utilizării sau accesării datelor.

2. Asigurarea securității datelor personale

În funcție de specificul activității, dimensiunea și resursele organizației, se iau o serie de măsuri tehnice menite să securizeze datele personale.

A. Protejarea sistemelor și aplicațiilor cu parole, sisteme antivirus, anti spyware, anti malware etc., sistem de schimbare a parolelor periodic;

B. Utilizarea aplicațiilor și programelor licențiate și actualizate conform recomandărilor producătorilor;

C. Auditarea periodică a sistemelor IT;

D. Criptarea corespondențelor;

E. Securizarea dulapurilor și locurilor de depozitare a dosarelor care conțin date personale

3. Ce trebuie să facă ONG-ul în caz de incident de securitate

Trebuie să investigheze foarte rapid cauzele și contextul incidentului și să îl documenteze:

(a) să descrie caracterul 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;

(c) să descrie consecințele probabile ale încălcării securității datelor cu caracter personal;

[1] Art. 33-34 GDPR.

(d) să descrie măsurile luate sau propuse spre a fi luate pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

Pentru a putea îndeplini această obligație este necesar ca procedura internă a ONG-ului să prevadă pașii de urmat în cazul identificării unui incident. Pentru aceasta sunt necesare:

- Instruiri periodice cu angajații/persoanele implicate în prelucrare ca aceștia să poată recunoaște un incident;
- Indicarea pașilor de urmat în cazul identificării incidentului: pe cine anunță, ce măsuri iau etc.
- Persoana responsabilă pentru notificarea Autorității de Supraveghere
- Aceste proceduri și cunoașterea lor au rolul de a asigura respectarea termenului scurt de 72 de ore care se calculează de la momentul la care orice persoană de sub autoritatea operatorului a aflat (sau trebuia să afle în mod rezonabil) că s-a produs un incident.

ONG-ul păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse.

În cazul în care în urma investigației interne rapide **rezultă că încălcarea este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice**[2], atunci **trebuie notificată Autoritatea de supraveghere (ANSPDCP) în termen de 72 de ore**. Dacă riscurile sunt ridicate, atunci trebuie notificate și persoanele fizice.

[2] Riscul se apreciază de la caz la caz. Instrumente utile pentru apreciere a riscului - Ghidul European Data Protection Board (https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2021/guidelines-012021-examples-regarding-data-breach_en)

VII. Resurse suplimentare

Legislație

1. Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului 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)**

2. Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului general privind protecția datelor

Instituții publice relevante și publicații

1. European Data Protection Board (https://edpb.europa.eu/edpb_en)

2. European Data Protection Supervisor (https://edps.europa.eu/_en)

   • Factsheets: https://edps.europa.eu/press-publications/publications/factsheets_en

3. Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (**www.dataprotection.ro**)

   • Întrebări frecvente: https://www.dataprotection.ro/?page=IntrebariFrecvente

   • Noul Regulament General de Protecția Datelor – informații și instrumente utile: https://www.dataprotection.ro/?page=noua%20_pagina_regulamentul_GDPR

Ghiduri adoptate de Grupul de Lucru art. 29 cu privire la GDPR și aprobate de Comitetul European pentru Protecția Datelor

1. Orientări privind consimțământul în temeiul Regulamentului 2016/679

2. Orientări privind transparența în temeiul Regulamentului 2016/679

3. Orientări privind notificarea încălcării securității datelor cu caracter personal în temeiul Regulamentului 2016/679

Alte resurse

1. GDPR checklist for data controllers - https://gdpr.eu/checklist/

2. European Center for Nont-for-profit Law (ECNL) - Data Protection Standards for Civil Society Organisations

3. Open Society Foundation - Civil Society Organizations and General Data Protection Regulation Compliance: Challenges, Opportunities, and Best Practices

4. Asociația Specialiștilor în Confidențialitatea și Protecția Datelor - GHID pentru prelucrarea datelor cu caracter personal de către ONG-uri în cadrul campaniilor de strângere de fonduri

Semilunei nr 7, apt 1
București, Sector 2
www.expertforum.ro