Ghid GDPR pentru ONG-uri

GLOSAR

„GDPR", „Regulamentul" - REGULAMENTUL (U.E.) 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, în limba engleză General Data Protection Regulation).

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

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

„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.

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

„destinatar” - înseamnă 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. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării.

„parte terță” - înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal.

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

„încălcarea securității datelor cu caracter personal” - înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea.

„reprezentant” - înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator în temeiul articolului 27 din GDPR, care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile care le revin în temeiul GDPR.

„reguli corporatiste obligatorii” - înseamnă politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce privește

transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe țări terțe în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună.

„autoritate de supraveghere” - înseamnă o autoritate publică independentă instituită de un stat membru în temeiul articolului 51 GDPR.

„DPO” - responsabilului cu protecția datelor (în limba engleză *data protection officer*).

„DPIA” - Evaluarea impactului asupra protecției datelor (în limba engleză *data protection impact assessment*, acronim: DPIA).

„ONG” - organizațiile neguvernamentale sunt persoane juridice constituite de persoane fizice sau persoane juridice care urmăresc desfășurarea unor activități în interes general sau în interesul unor colectivități locale ori, după caz, în interesul lor personal nepatrimonial.

Ghid GDPR pentru ONG-uri

I. Introducere

***Aspecte introductive**

Prezentul Ghid ar trebui să reprezinte o lectură esențială pentru cei care sunt responsabili de protejarea datelor cu caracter personal privind activitățile unei organizații neguvernamentale. Ghidul este un instrument util pentru o organizație de a-și dezvolta cunoștințele sale în probleme legate de protecția datelor cu caracter personal. Acest Ghid își propune ca obiectiv să vă ajute să înțelegeți realitățile practice ale Regulamentului nr. 679/2016 (GDPR) și cum acesta va avea impact asupra modului dumneavoastră de lucru. Este important ca organizațiile non-profit și, prin extensie, board-ul acestora, personalul și voluntarii să înțeleagă importanța redactării și implementării unor proceduri și politici GDPR excelente pentru organizație. A proceda în sens contrar ar putea avea ca rezultat producerea unor riscuri financiare și reputațiunile considerabile pentru ONG.

Se adresează tot mai des întrebarea dacă GDPR este obligatoriu să fie respectat și de către organizațiile non-profit atâta vreme cât acestea fac activități din care nu rezultă profit?

Răspunsul este afirmativ. GDPR nu ține cont de entitate și nu există niciun fel de derogare de la respectarea acestui regulament european de către ONG-uri. GDPR trebuie respectat și de ONG-uri atâta vreme cât lucrează cu date personale.

Prin natura sa, o asociație sau fundație foarte rar nu va lucra cu date personale. Astfel de entități au de regulă oameni care donează, și legea impune ținerea unei evidențe a donatorilor și transmiterea acestei evidențe către autorități, și mai are oameni care fac voluntariat și care nu sunt anonimi. Voluntarii au un regim special, fiind asimilați angajaților, au nevoie de contract de voluntariat, protecția muncii etc.

O altă categorie de date apare când ONG-ul lucrează pentru oameni din diferite comunități, cum ar fi copiii, de la care le culege datele pentru a-i putea ajuta, persoane pentru care fac strângeri de fonduri, adulți din categorii discriminate sau defavorizate și altele, când adesea se lucrează cu cele mai sensibile date cu caracter personal.

La fel și ONG-urile care fac cursuri de orice fel unde oamenii se înscriu cu date personale pentru a primi diplome și certificări, fie ele acreditate sau neacreditate.

Mai mult, GDPR se aplică **și paginilor web**. Website-urile, fie ele de prezentare, de donații sau magazine, prin care își adună fonduri trebuie să fie aliniate cu legislația. În acest sens trebuie să vă creați cel puțin trei pagini: Politică despre cookie-uri, Politică de confidențialitate și Termeni și condiții. Paginile de Facebook, dacă acestea colectează date, trebuie și ele incluse în politica de confidențialitate a datelor cu caracter personal pe care ONG-ul este obligat să o întocmească.

În consecință, și ONG-urile trebuie să se alinieze legislației privind protecția datelor cu caracter personal și nu sunt deloc scutite de controale sau amenzi mai ales pentru că, prin natura activității, lucrează cu mulți oameni ca voluntari, poate cu oameni care activează doar o lună sau o perioadă limitată, care au acces la date cu caracter personal.

Faptul că un ONG poate rula mulți voluntari e un motiv în plus să aibă politici foarte bune.

Nu neglijați acest aspect, ci creați politici de protecție a datelor pe baza legislației în vigoare și a analizelor proprii efectuate, pentru a oferi în mod efectiv o protecție a datelor cu caracter personal, fie că vorbim despre voluntarii implicați sau de beneficiarii activităților organizației non-profit.

****Principii fundamentale prevăzute de GDPR**

Principiul minimizării datelor – Solicitați și prelucrați strict datele de care aveți nevoie. *De exemplu*, dacă pentru înscrierea la un eveniment aveți nevoie doar de datele de contact, nu solicitați și informații precum starea civilă sau situația profesională.

Principiul accesului limitat la date – La datele cu caracter personal deținute de organizație trebuie să aibă acces doar cei care au cu adevărat nevoie de ele. Aici este important de organizat accesul digital și fizic la datele cu caracter personal doar pentru angajații și voluntarii care chiar trebuie să opereze cu ele, dar și să limitați/eliminați accesul imediat ce persoana respectivă nu mai face parte din organizație sau părăsește proiectul.

Principiul eficientizării datelor – Este important să știți ce date colectați, unde le stocați, cine are acces la ele. Un exercițiu de reflecție în cadrul ONG-ului ar fi foarte util, indiferent dacă doar trimiteți un newsletter sau gestionați voluntari.

Informarea beneficiarilor – Cei cărora li se procesează datele cu caracter personal trebuie să fie întotdeauna informați. Creați o Politică a Datelor cu Caracter Personal, într-un limbaj simplu, care să cuprindă: ce date sunt colectate, unde sunt acestea stocate, în ce scopuri sunt folosite (cât mai specific), pe ce durată se colectează, cine are acces la ele, ce drepturi au proprietarii datelor respective.

Folosirea bazei legale pentru procesarea datelor – Colectarea și procesarea datelor se face strict folosind una dintre bazele legale menționate de GDPR. Consimțământul este doar una dintre acestea. Bazele legale sunt detaliate mai jos. Important este să identificați în fiecare situație ce bază legală utilizați pentru prelucrarea datelor cu caracter personal.

Transferul datelor – Atunci când transferați date cu caracter personal către alte organizații este important să aveți clauze contractuale referitoare la protecția datelor personale. De asemenea, când transferul are loc către o altă țară, trebuie să verificați

dacă țara în cauză asigură un nivel adecvat de protecție a datelor personale. Asta implică și datele stocate pe servere din alte țări, precum SUA (Dropbox, Google Drive etc). SUA nu este considerată o țară la fel de sigură ca UE pentru protecția datelor personale.

Data Protection Officer – Este necesar numai în anumite situații specifice. Mai exact, dacă prelucrați date sensibile sau dacă gestionați date cu caracter personal în masă și le prelucrați (pentru un număr mare de oameni).

Ghid GDPR pentru ONG-uri

*****Care sunt pașii de urmat din perspectiva GDPR pentru ONG-ul dumneavoastră?**

Vă recomandăm să luați următoarele măsuri pentru respectarea măsurilor impuse de GDPR:

- ✓ Realizați un „audit" al datelor personale în cadrul organizației. Verificați, împreună cu echipa, ce date sunt colectate/folosite, unde se află acestea, cine are acces la ele.
- ✓ Asigurați-vă că folosiți aplicații digitale pe conturi ale ONG-ului, și nu pe cele personale. De exemplu, ca ONG aveți acces gratuit la Google for Nonprofits sau Office 365 for Nonprofits. Înscrieți-vă și folosiți-le, pentru că asta înseamnă că semnați acorduri/contracte cu acești furnizori inclusiv pentru GDPR, având astfel o grijă în minus. De asemenea, verificați dacă datele se află pe conturile digitale ale organizației. Când acestea ajung pe conturi personale pot fi vulnerabile în fața unui „data breach" (inclusiv copierea datelor de către un voluntar pentru uz propriu, de exemplu, sau transferul neautorizat către un alt ONG) de care nu doriți să auziți.
- ✓ Întocmiți o Politică a Protecției Datelor Personale a ONG-ului dumneavoastră, într-un limbaj cât mai simplu, și publicați-o la loc vizibil pe website. Apoi puteți include un link către aceasta în formularele online, liste de semnături etc.
- ✓ Actualizați formularele din organizație, în special cele legate de înscrierea la evenimente, la newslettere, liste de participanți. Asigurați-vă că solicitați consimțământul atunci când acesta este necesar și că informați în permanență beneficiarii cu privire la datele lor cu caracter personal pe care le dețineți. Nu este cazul de exces de zel, fiind suficientă o bifă clară cu scopul prelucrării datelor și link către politica dumneavoastră de prelucrare.
- ✓ Dacă vi se pare util puteți crea mici proceduri interne pentru diferite situații (ce faceți când cineva își retrage consimțământul sau solicită ștergerea datelor, de exemplu).
- ✓ Asigurați-vă că accesul la date este exercitat doar de către persoane autorizate. Setați permisiunile din Google Drive/Dropbox/pagina de Facebook și unde mai este necesar, acordând în special atenție celor care nu mai fac parte din organizație, dar continuă să aibă acces.

- ✓ Informați echipa ONG-ului cu privire la schimbările GDPR, atât la nivel managerial/operațional, cât și beneficiarii.

GDPR aduce cu siguranță provocări majore pentru orice ONG, dar dacă privim aceste schimbări ca pe un imbold înspre eficientizare și profesionalizare, putem constata că, până la urmă, GDPR a sprijinit întregul demers. Datele pe care le avem în grijă sunt responsabilitatea noastră și este bine să le protejăm așa cum ne-am aștepta și noi să ne fie protejate datele cu caracter personal de către alte organizații.

II. Analiza activităților de prelucrare a datelor cu caracter personal de către ONG-uri

Organizațiile neguvernamentale sunt structuri instituționalizate de natură privată ce pot activa fie ca grupuri informale, fie ca persoane juridice, și care sunt independente în raport cu orice autoritate publică. Ele nu urmăresc nici accesul la puterea politică și nici obținerea de profit.

Din punct de vedere juridic, în România, organizațiile neguvernamentale pot exista sub trei forme: asociație, fundație, federație. În ceea ce privește denumirile comerciale, în practică se întâlnește o largă varietate de denumiri: club, comitet, societate, confederație etc.

Spre deosebire de societățile comerciale, organizațiile neguvernamentale obțin, de obicei, cea mai mare parte a veniturilor prin sponsorizări, donații sau finanțări nerambursabile (granturi) și mai rar prin activități economice cu caracter profitabil.

Organizațiile neguvernamentale se bazează, în general, pe activități voluntare în procesul de conducere (activitatea consiliului de administrație nu este remunerată) sau în acțiunile pe care le desfășoară (dar utilizarea de voluntari nu exclude posibilitatea angajării de personal). Aceste elemente se regăsesc în funcționarea organizațiilor, indiferent de țara în care activează.

Organizațiile neguvernamentale sunt caracterizate printr-o mare mobilitate în ceea ce privește modul și direcțiile lor de acțiune. Această mobilitate reprezintă condiția lor de supraviețuire, atâta vreme cât funcționarea lor este dependentă de o corectă identificare a nevoilor în comunitate și de atragerea resurselor necesare pentru abordarea acestor nevoi. Organizațiile neguvernamentale reprezintă un „barometru” al comunității.

Ghid GDPR pentru ONG-uri

Organizațiile neguvernamentale sunt active în orice domeniu în care se manifestă nevoia societății: **educație, știință, cercetare, cultură, protecție socială, minorități, drepturile omului, protecția mediului, protecția copilului etc.**

În acest sens, organizațiile neguvernamentale își pot asuma diverse funcții, cum ar fi:

- Intermedierea relației dintre cetățeni și autorități
- Facilitarea integrării sociale și politice a cetățenilor (organizațiile reprezintă un cadru de participare civică)
- Furnizarea de bunuri și servicii publice
- Reprezentarea intereselor de grup în societate.

ONG, în respectarea principiului bunei guvernări, poate ajunge să prelucreze o cantitate mare de date cu caracter personal raportat la toți actorii interesați: **beneficiarilor, partenerilor, autorităților locale sau centrale, finanțatorilor, reprezentanților media trebuie să li se ofere, ușor și accesibil, informații complete privind activitățile organizației, aceasta fiind principala cale de a obține credibilitatea și suportul necesare succesului acestor activități.**

Categorii de date cu caracter personal. Ce date cu caracter personal prelucrați?

GDPR definește datele personale ca fiind orice informație/dată care poate duce la identificarea unei persoane fizice, prin orice mijloace. Includem aici nu doar datele evidente precum numele sau CNP-ul, ci și date precum IP-ul folosit pentru a accesa website-ul organizației.

Există și date cu caracter sensibil, cum ar fi cele despre starea de sănătate sau cele biometrice (amprente, iris, imaginea facială – atenție la copiile de buletin!).

Iar ONG-ul dumneavoastră prelucrează date personale, ca aproape orice persoană juridică, deci intră complet sub incidența GDPR. Datele cu caracter personal prelucrate de către un ONG pot fi: datele membrilor, beneficiarilor, voluntarilor, board-ului, datele persoanelor înscrise la newslettere, datele vizitatorilor paginilor web, datele vizitatorilor

paginii de Facebook, datele angajaților, datele suporterilor, datele participanților la un eveniment, datele finanțatorilor instituționali sau asociativi, datele partenerilor etc.

Explicat într-un mod mai structurat, datele personale pot fi orice date:

- **ale** persoanei vizate (nume, prenume, CNP, amprentă, ADN)
- **despre** persoana vizată (vârstă, sex, etnie, rasă, orientare sexuală, politică, religioasă, starea de sănătate)
- **în legătură cu** persoana vizată (adresa de domiciliu, reședința, adresa de e-mail, ocupația, venitul).

Care, singure sau cumulate, ar putea identifica o persoană – adică orice alte tipuri de date care se pot corela pentru a conduce la identificarea unei persoane vizate.

Temeiuri legale pentru prelucrarea datelor cu caracter personal

Prelucrarea datelor cu caracter personal se poate realiza în mod legal numai dacă se bazează pe unul dintre temeiurile juridice prevăzute la art. 6 alin. (1) din Regulament, respectiv:

a) **consimțământul** persoanei vizate;
b) prelucrarea este necesară pentru **încheierea sau executarea unui contract**;
c) prelucrarea este necesară pentru îndeplinirea **unei obligații legale**;
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 învestit 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.

Sunt necesare câteva precizări privind selectarea temeiului juridic de prelucrare adecvat fiecărei categorii de prelucrare de date cu caracter personal:

a) ținând cont de scopurile urmărite prin prelucrarea datelor cu caracter personal, primul pas în evaluarea conformității unei prelucrări de date este determinarea temeiului juridic în baza căruia se face prelucrarea. Fără un temei juridic corect identificat, prelucrarea este ilegală;

b) alegerea temeiului de prelucrare trebuie făcută corect de la început, schimbarea ulterioară a temeiului, fără justificare adecvată, este echivalentă cu o neconformitate;

c) alegerea temeiului de prelucrare trebuie documentat *(cel mai frecvent, prin evidența activităților de prelucrare);*

d) persoanele vizate trebuie informate cu privire la temeiul prelucrării, ca principiu, înainte de începerea prelucrării.

➢ Prelucrare pe bază de consimțământ [Art. 6 alin. (1) lit. (a) din Regulament]

În lumina noilor prevederi ale Regulamentului, prelucrarea datelor pe bază de consimțământ presupune respectarea unor standarde legale specifice. A prelucra date pe baza consimțământului înseamnă a da persoanei vizate reală libertate de alegere și control sporit asupra prelucrării. Enumerăm, mai jos, câteva dintre cele mai importante reguli de obținere și gestionare a consimțământului:

a) Consimțământ **explicit.** Consimțământul trebuie să fie exprimat în mod explicit, într-o manieră clară și specifică (manifestare pozitivă a consimțământului). Utilizarea unor metode de exprimare implicită/tacită a consimțământului (spre exemplu, căsuțe de acord pre-bifate) nu este o practică legală.

b) Consimțământ **nelegal**. Furnizarea unui serviciu solicitat de/oferit persoanei vizate nu poate fi condiționată de acordarea consimțământului pentru prelucrare din partea respectivei persoane, întrucât astfel, consimțământul nu ar fi liber exprimat.

c) Consimțământ **separat.** Consimțământul trebuie solicitat (i) în mod separat de termeni și condiții ori alte documente de informare și prezentare și (ii) în mod specific pentru fiecare scop pentru care se face prelucrare pe acest temei juridic.

d) Consimțământ **documentat.** Consimțământul trebuie documentat și dovada acestuia trebuie păstrată. Ca principiu, operatorul trebuie să poată demonstra cine

a dat consimțământul, când, prin ce metodă și ce informații au fost furnizate cu ocazia preluării consimțământului.

e) Consimțământ **revocabil.** Persoana vizată are dreptul de a retrage consimțământul în orice moment (formă de manifestare a „dreptului de a fi uitat"), iar operatorul trebuie să ofere un mecanism de retragere facil și să acționeze pentru a da eficiență retragerii în cel mai scurt timp posibil.

Acest set de reguli face ca prelucrarea pe bază de consimțământ să ridice numeroase probleme practice. De aceea, trebuie să răspundeți în primul rând la întrebarea dacă consimțământul este într-adevăr temeiul juridic adecvat prelucrărilor de date cu caracter personal pe care doriți să le realizați sau există un alt temei juridic mai potrivit. Determinarea este cu atât mai importantă cu cât alegerea temeiului juridic este unică și, în principiu, nu poate fi schimbată ulterior începerii prelucrării.

În activitatea dumneavoastră, prelucrările de date având ca temei consimțământul persoanei vizate pot fi cele mai numeroase. Prelucrarea datelor persoanelor vizate nu se bazează întotdeauna pe temeiul necesității încheierii sau executării unui contract *(așa cum vom arăta în continuare)*. De exemplu, prelucrarea datelor angajaților, persoane fizice, în scop de marketing *(transmiterea de alerte/newslettere prin e-mail)* va trebui să aibă la bază un consimțământ obținut în mod legal de la aceștia.

Prin urmare, trebuie să existe forme de **comunicare activă** în cazul în care se invocă consimțământul persoanei vizate. În timp ce consimțământul vă poate oferi un temei în sensul prelucrării datelor cu caracter personal, semnalăm că nu este întotdeauna posibilă o asemenea ipoteză sau chiar de dorit. Dacă aveți de gând să vă bazați pe consimțământul persoanei vizate, trebuie să vă asigurați că aceste persoane știu exact ce fel de date veți prelucra și că înțeleg implicațiile asupra lor. Ele trebuie să cunoască dacă este sau nu necesară prelucrarea. *Nu trebuie să condiționați furnizarea unui serviciu de obținerea consimțământului persoanei vizate.*

Spre exemplu, operatorul de date cu caracter personal trebuie să obțină consimțământul în situația în care intenționează să comunice informații/oferte personalizate cu privire la

produse, servicii și activități ale organizației non-profit (marketing direct) sau pentru efectuarea studiilor de marketing, dacă este cazul.

De asemenea, consimțământul trebuie să fie întotdeauna pe principiul „opt-in", adică utilizatorul alege să îi fie colectate datele (să primească un newsletter, de exemplu), în niciun caz „opt-out", unde presupunem că putem lua datele și dacă utilizatorul nu e de acord se va dezabona. Acordul poate fi demonstrat prin orice mijloace (click, bifarea unei căsuțe, semnătură).

Important! ONG-urile nu vor avea nevoie de consimțământul persoanelor cărora le prelucrează datele personale pentru activitățile aferente îndeplinirii obiectivelor sale, sub condiția instituirii unor garanții corespunzătoare, conform dispozițiilor **art. 9 din 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).*

Orice categorii de date ar prelucra, chiar și chestiuni care s-ar încadra cu succes în categoria datelor sensibile, legea le permite organizațiilor non-profit prelucrarea lor fără consimțământ, cu toate că legislația europeană în materia protecției datelor personale, cea pe care se presupune că acest act normativ o pune în aplicare, indică altceva.

Se prevede însă că organizațiile non-profit vor trebui să ofere anumite garanții celor cărora le prelucrează datele, cum ar fi **informarea lor** despre prelucrările de date:

- *"**Prelucrarea datelor cu caracter personal şi 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**".*

Obținerea consimțământului nu va fi necesară, după cum se observă din textul citat mai sus, nici pentru prelucrarea acelor categorii speciale de date. Cu toate că, la acest capitol, GDPR prevede că prelucrarea unor astfel de date speciale ar trebui să se facă numai în situații de excepție.

Totuși, este important de menționat că, deși legea națională nu menționează acest lucru, GDPR prevede clar, în **art. 9 alin. (2) lit. d) din Regulament,** că datele speciale pot fi prelucrate de ONG fără consimțământ **doar dacă** se referă la membri sau la foști membri sau la persoane cu care există contacte permanente în legătură cu scopurile sale și că aceste date nu pot fi comunicate terților fără consimțământul persoanelor vizate. *De aici rezultă că pot fi prelucrate fără consimțământ doar datele speciale relevante față de scopul acelei organizați.*

Derogarea permisă ONG-urilor nu este generală, ci acestea trebuie să respecte în continuare toate celelalte reguli în materia prelucrării de date personale prevăzute la **art. 5 din Regulament** *(informarea, limitarea la scop, minimizarea, exactitatea, securitatea, limitarea duratei de stocare, responsabilitate).*

Garanțiile pe care ONG-urile ar trebui să le ofere celor cărora le prelucrează datele sunt:

- *informarea persoanei vizate despre prelucrarea datelor cu caracter personal;*
- *garantarea transparenței informațiilor, a comunicărilor și a modalităților de exercitare a drepturilor persoanei vizate;*
- *garantarea dreptului la rectificare și ștergere.*

Nu sunt prevăzute însă mai multe detalii cu privire la aplicarea acestor garanții, care sunt, de fapt, chestiuni la care GDPR-ul obligă oricum. *De exemplu*, entitățile care prelucrează datele personale trebuie să ofere, ca regulă, respectarea dreptului la ștergerea ori rectificarea datelor atunci când persoanele vizate le cer aceste lucruri. Așadar, orice persoană ale cărei date sunt prelucrate de ONG-uri ar trebui informată despre prelucrare.

- **Prelucrare necesară pentru încheierea și executarea unui contract [art. 6 alin. (1) lit. (b) din Regulament]**

Elementul-cheie care justifică utilizarea acestui temei juridic este necesitatea încheierii sau executării unui contract. În acest context, prelucrarea este legală dacă:

a) există un contract valabil, pentru a cărui executare este necesară prelucrarea de date cu caracter personal; sau

b) în faza pre-contractuală, la solicitarea persoanei vizate, este nevoie de prelucrarea anumitor date cu caracter personal în vederea încheierii contractului.

În mod contrar, prelucrarea NU se poate baza pe temeiul încheierii/executării contractului dacă:

a) trebuie prelucrate datele unei persoane, alta decât cea cu care se încheie contractul;

b) inițiativa încheierii contractului vă aparține sau aparține unei terțe persoane.

Cerința necesității prelucrării pentru încheierea sau executarea unui contract nu înseamnă întotdeauna că prelucrarea este esențială în acest scop, totuși aceasta trebuie să fie limitată la și proporțională cu scopul urmărit.

Spre exemplu, o persoană se înscrie ca membru într-un club, ulterior datele sale sunt folosite pentru a intra în baza de date a membrilor, iar prelucrarea datelor are loc conform așteptărilor beneficiarului și ca urmare a înscrierii ca membru - temeiul legal de prelucrare ar putea fi reprezentat de încheierea/executarea unui contract pentru ambele operațiuni. Dacă datele cu caracter personal ale membrului sunt utilizate în alte scopuri decât cel inițial – *înscrierea ca membru* – va trebui identificat un temei de prelucrare suplimentar.

- **Prelucrare necesară pentru îndeplinirea unei obligații legale [art. 6 alin. (1) lit. (c) din Regulament]**

Prelucrarea datelor cu caracter personal pe temeiul necesității conformării unei obligații legale presupune existența unor norme legale care vă sunt aplicabile. De asemenea, prelucrarea impusă printr-o decizie administrativă/hotărâre judecătorească (ele însele luate în temeiul unei abilitări legale) poate fi justificată tot prin necesitatea conformării unei obligații legale.

Spre exemplu:

- furnizarea informațiilor necesare pentru calcularea și reținerea taxelor ce țin de plățile salariale aferente angajaților: primele de asigurare obligatorie de asistență medicală, contribuțiile la bugetul asigurărilor sociale de stat, impozitul pe venit etc.
- întocmirea și păstrarea documentelor financiar-contabile (chitanțe, facturi etc.)

Prelucrarea trebuie să fie necesară conformării obligației legale. Dacă se poate asigura în mod rezonabil conformarea cu norma legală fără respectiva prelucrare sau printr-o prelucrare mai puțin invazivă/cuprinzătoare, nu poate fi utilizat acest temei.

Prelucrarea datelor care se desfășoară pentru îndeplinirea unor obligații legale nu necesită altceva decât informarea beneficiarilor. *De exemplu*, puteți fi obligați să oferiți copii după cărțile de identitate ale participanților pentru a valida o anumită finanțare publică.

Atenție! Aici vorbim inclusiv de legislația europeană, cum ar fi Regulamentul Erasmus+, ce conține prevederi clare referitoare la protecția datelor personale și situațiile în care prelucrarea acestora de către ONG este obligatorie. Aici poate intra și arhivarea sau stocarea pentru a demonstra unui finanțator anumite informații în caz de audit.

- **Prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice [art. 6 alin. (1) lit. (d) din Regulament].**

Folosiți această bază legală atunci când este o situație de viață și de moarte, moment în care nu ar mai fi necesară nicio altă justificare suplimentară. Se va putea proceda imediat la orice intervenție indispensabilă din punct de vedere medical în folosul sănătății persoanei vizate, situație în care apreciem că temeiul legal analizat este pe deplin aplicabil pentru prelucrarea datelor cu caracter personal de către ONG-uri.

- **Prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul [art. 6 alin. (1) lit. (e) din Regulament].**

Acest temei operează atunci când prelucrarea datelor personale ale unei persoane este necesară pentru îndeplinirea unei sarcini de interes public. Deși ONG-urile nu reprezintă o *„autoritate/instituție publică”,* totuși se poate aprecia că cele pentru care le-a fost recunoscută utilitatea publică, conform legii, își desfășoară activitatea în interes public în funcție de domeniul în care activează.

În plus, prin dispozițiile **art. 2 din 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) este definită sintagma ***„îndeplinirea unei sarcini care servește unui interes public”,*** incluzând acele **activități** ale partidelor politice sau ale organizațiilor cetățenilor aparținând minorităților naționale, **ale organizațiilor neguvernamentale**, care servesc realizării obiectivelor prevăzute de dreptul constituțional sau de dreptul internațional public ori funcționării sistemului democratic, incluzând încurajarea participării cetățenilor în procesul de luare a deciziilor și a pregătirii politicilor publice, respectiv promovarea principiilor și valorilor democrației.

Acest temei legal de prelucrare este pe deplin aplicabil activităților de prelucrare realizate de ONG-urile cărora li s-a recunoscut în mod legal **statutul de utilitate publică.**

Rețineți faptul că acest temei legal de prelucrare este incident **doar în cazul datelor cu caracter personal obișnuite** (nume, prenume, număr de telefon, adresă de e-mail etc.), **nu și în privința celor speciale** (privind sănătatea, date genetice, biometrice, spre exemplu), pentru prelucrarea cărora este necesară identificarea unuia dintre temeiurile de prelucrare prevăzute la art. 9 alin. (2) din Regulament.

- **Prelucrare necesară în scopul realizării unui interes legitim [art. 6 alin. (1) lit. (f) din Regulament]**

Interesul legitim este cel mai flexibil temei juridic de prelucrare a datelor cu caracter personal și, de aceea, utilizarea sa trebuie calibrată în mod adecvat. În mod tipic, poate fi folosit doar în cazurile în care prelucrarea are un impact minimal asupra persoanelor vizate. Pentru o judicioasă întemeiere pe interesul legitim, prelucrarea datelor cu caracter personal trebuie să îndeplinească trei tipuri de caracteristici:

a) Testul **scopului legitim**. Trebuie să urmăriți un interes legitim, al dumneavoastră sau al unui terț. Interesul legitim poate fi un interes comercial, profesional sau un scop mai larg, de exemplu un interes social.

b) Testul **necesității.** Prelucrarea trebuie să fie proporțională și limitată pentru atingerea interesului legitim urmărit. Dacă respectivul interes poate fi atins printr-o prelucrare mai puțin intruzivă/cuprinzătoare, nu poate fi utilizat acest temei.

c) Testul **raportării la interesele persoanei vizate**. Ca principiu, prelucrarea trebuie să fie previzibilă pentru persoana vizată și să nu creeze un prejudiciu/ inconvenient persoanei vizate.

Exemplu de interes legitim: O organizație non-profit poate să se bazeze pe interes legitim pentru a justifica analiza datelor cu caracter personal în vederea determinării strategiei sale operaționale și să-i permită să hotărască asupra potențialilor beneficiari de servicii.

În consecință, apreciem că prelucrările pe care le efectuați pot avea ca temeiuri legale de prelucrare: **consimțământul** persoanei vizate (datele prelucrate în contextul transmiterii de newslettere, datele prelucrate în contextul organizării unor evenimente), **încheierea/executarea unui contract** încheiat cu persoanele vizate *(parteneri, colaboratori, angajați etc.),* **respectarea/îndeplinirea unei obligații legale** *(prelucrarea datelor necesar a fi menționate în cuprinsul documentelor justificative – facturi, chitanțe, îndeplinirea unei cerințe legale specifice etc.).*

Cu toate acestea, rețineți faptul că într-o anumită ipoteză pot fi incidente două temeiuri legale de prelucrare a datelor cu caracter personal – îndeplinirea unei obligații legale și/ executarea unui contract, raportarea la cel mai potrivit temei urmând a se efectua în funcție de circumstanțele concrete ale situației de fapt.

De asemenea, ca temei legal de prelucrare a datelor cu caracter personal care ar putea fi incident în activitățile specifice organizațiilor non-profit menționăm și **interesul legitim** al operatorului (art. 6 alin. (1) lit. f) din Regulament). Spre exemplu, în cazul *monitorizării video.*

În acest sens, va trebui să analizați, să stabiliți și să documentați temeiul legal care stă la baza prelucrării datelor cu caracter personal, **în funcție de particularitățile fiecărei activități de prelucrare a datelor cu caracter personal.**

Prelucrarea de categorii speciale de date cu caracter personal

Regulamentul definește categoriile speciale de date: originea rasială sau etnică, opiniile politice, confesiunea religioasă, convingerile filozofice, apartenența la sindicate, date genetice, date biometrice pentru identificarea unică a unei persoane fizice, date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice.

Aceste categorii de date sunt considerate sensibile și se impune un standard de protecție superior.

ONG-urile prelucrează astfel de date cu caracter personal (speciale), dintre care menționăm exemplificativ: date privind originea rasială sau etnică, apartenența la sindicate, date privind sănătatea, datele biometrice (imaginile surprinse de camerele video), dacă se reține copii ale CI (imaginea din cuprinsul CI), informații cu privire la expunerea politică a unei persoane, seriile și numărul actelor de identitate (date ce identifică unic o anumită persoană fizică) etc.

Concret, pentru prelucrarea adecvată a acestor categorii de date, este important să rețineți că **pe lângă identificarea unui temei de prelucrare potrivit art. 6 din Regulament, se impune îndeplinirea și a unuia dintre temeiurile legale de prelucrare reglementate de art. 9 alin. (2) din Regulamentul nr. 679/2016 aplicabile pentru categoriile de date cu caracter special**:

a) **consimțământul explicit** al persoanei vizate;

Cum este practic exprimat acest acord expres? Consimțământ expres exprimat, înseamnă că persoana vizată a înțeles cum vor fi prelucrate datele din aceste categorii, la cine vor ajunge și pentru ce scop. Dacă nu există transparență cu privire la aceste informații, nici persoana nu își poate da un acord valabil și cuprinzător. *„Accept termenii și condițiile”* bifând o căsuță, din punctul nostru de vedere, nu înseamnă un acord exprimat expres și în cunoștință deplină de cauză.

b) 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;

Ca angajator aveți nevoie să respectați obligațiile specifice domeniului dreptului muncii, de exemplu înregistrarea angajatului în sistemul ReviSal. Pentru ca obligațiile pentru protecția datelor personale să nu contrazică prevederile din dreptul muncii este nevoie de

această excepție. Cu toate acestea, sfătuim să nu se ceară la angajare mai multe date personale decât este strict necesar (*de exemplu, pentru angajarea într-un call center nu ar trebui să solicitați detalii despre viața sexuală a angajatului*). Mai mult, indiferent de datele pe care le prelucrați ca angajator este interzis a divulga datele pe care le colectați unei alte companii, instituții, organizații, asociații.

Pot exista cazuri când aveți o obligație legală în calitate de operator să transmiteți mai departe datele cu caracter personal (de exemplu unei instituții/autorități publice - ANAF) sau dacă persoana vizată și-a dat acordul expres că puteți dezvălui datele cu caracter personal.

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;

În alte cuvinte, dacă nu se realizează prelucrarea, viața, integritatea fizică sau sănătatea unei persoane (ori a persoanei în cauză, ori a altei persoane) ar putea fi afectate sau puse în pericol. Sau dacă persoana în cauză nu își poate exprima consimțământul – poate fi un motiv de ordin fizic (de exemplu din motive medicale) sau juridic (exemplu este o persoană sub 18 ani – 18 ani fiind vârsta legală în România pentru dobândirea capacității depline de exercițiu).

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*;

De exemplu, un scop legitim este atunci când o organizație non-profit pentru promovarea drepturilor sexuale și ale reproducerii reprezintă în instanță o persoană care consideră că i-au fost încălcate drepturile, iar reprezentarea în instanță a persoanelor

vulnerabile face parte din activitățile cuprinse în statutul organizației. Condiția esențială pentru prelucrarea legitimă a datelor speciale este ca persoana vizată să fie membră a acelei organizații sau să aibă relații cu ONG-ul respectiv. În niciun caz datele nu pot fi dezvăluite terților fără consimțământul persoanei vizate.

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

Un exemplu este atunci când persoana respectivă are un blog public în care face dezvăluiri despre apartenența politică sau despre viața sa sexuală.

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;

h) **prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluare a 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. Condiția esențială este ca prelucrarea datelor să fie efectuate ori sub supravegherea unui cadru medical supus secretului profesional, ori sub supravegherea unei alte persoane supuse unei obligații echivalente în ceea ce privește secretul.

i) prelucrarea este necesară din motive de interes public în domeniul sănătății publice; sau

j) **prelucrarea este necesară** în scopuri de **arhivare** în interes public, în scopuri de cercetare științifică sau istorică ori **în scopuri statistice.**

În mod tipic, temeiul juridic în baza căruia veți putea prelucra categorii speciale de date este **art. 9 alin. (2) lit. (a), d), f), g), h) și j) din Regulament.**

Specific ONG-urilor, reținești faptul că temeiul legal de prelucrare a datelor cu caracter personal cu privire la membrii săi, cu privire la foști membri sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale este reprezentat de art. 9 alin. (2) lit. d) din Regulament.

Dacă alegeți să vă întemeiați mare parte dintre prelucrările **datelor cu caracter personal speciale** pe acest temei legal de prelucrare, **atenție însă** la **dezvăluirea** datelor cu caracter personal ale categoriilor de persoane vizate menționate **către terți** *(entități distincte de operator/persoană împuternicită),* dezvăluire care **NU poate avea loc în lipsa consimțământului exprimat în mod expres de către persoanele vizate**.

Orice utilizare a acestor temeiuri legale va trebui **documentată (indicată în scris)**, operatorul de date cu caracter personal (organizația non-profit) având obligația de a justifica necesitatea oricărei prelucrări a **datelor cu caracter personal speciale.**

Temeiurile prelucrării datelor cu caracter personal din cuprinsul dispozițiilor art. 6 și 9 din RGPD se pot interschimba, în funcție de situația specifică fiecărei prelucrări. *Spre exemplu*, în momentul în care înregistrați datele biometrice prin intermediul camerelor CCTV, temeiul prelucrării va fi reprezentat de dispozițiile **art. 6 alin. (1) lit. f) din Regulament** - *prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță,* în vreme ce, temeiul legal de prelucrare a datelor cu caracter personal din categoria celor speciale ar putea fi cel de la **art. 9 alin. (2) lit. d) din Regulament** – *prelucrarea este efectuată în cadrul activităților lor legitime și cu garanţii 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*.

În lipsa unui temei legal de prelucrare a categoriilor de date cu caracter special prevăzut de GDPR în art. 9 alin. (2), datele cu caracter personal reglementate de art. 9 alin. (1) din Regulament nu ar trebui colectate/prelucrate în vreun fel.

2.1. Documentație de constituire și funcționare ONG. Temei legal de prelucrare

Prelucrările de date cu caracter personal efectuate cu prilejul organizării și funcționării ONG, indiferent că este vorba despre asociație, fundație/federație, apreciem că sunt efectuate în baza următoarelor temeiuri legale: **art. 6 lit. b), c), e) – dacă este cazul și art. 9 alin. (2) lit. d) din Regulament**, temeiuri stabilite în funcție de fiecare operațiune în parte. Avem în vedere întreaga documentație care a stat la baza acordării personalității juridice sau documentația în baza căreia funcționează entitatea și care conține date cu caracter personal.

Exemplificativ enunțăm: act constitutiv, hotărâri AGA, decizii, registru de procese-verbale, alte registre, liste de plată, rapoarte de activitate și orice alte documente de acest tip.

2.2. Strângerea de fonduri și GDPR

Activitatea de colectare a fondurilor s-a confruntat cu o criză de încredere. Utilizarea datelor donatorului a adus cu regularitate diverse critici la adresa celor care se ocupau cu strângerea de fonduri. **Introducerea GDPR are un impact semnificativ asupra modului în care ONG-urile atrag fonduri**. GDPR prezintă pentru dumneavoastră o mare oportunitate de revizuire a politicilor și procedurilor care să asigure respectarea absolută a lor raportat la diferite practici de strângere a fondurilor.

Având în vedere că în cele mai multe organizații non-profit departamentul de colectare de fonduri are cea mai mare interacțiune cu mediul extern, este foarte important ca liderii care se ocupă de strângerea de fonduri să se angajeze complet față de rigorile GDPR. Comunicarea cu donatorii și potențialii donatori este o activitate de specialitate. Este important să începeți cu cele mai bune practici de colectare a fondurilor și apoi să acordați atenție respectării GDPR, și nu viceversa.

De exemplu, ar trebui să interpretați la modul general reglementările GDPR cu privire la păstrarea datelor cu caracter personal, astfel încât să păstrați înregistrările pentru cea mai scurtă perioadă de timp posibil și proceduri de distrugere/ștergere a datelor cu caracter personal după doi ani ar putea fi create cu ușurință.

Cu toate acestea, este util să țineți unele date ale donatorului mai mult decât perioada pentru care donațiile se efectuează către organizația non profit. Cadourile testamentare apar de multe ori după mai mulți ani de tăcere a donatorului, cu atât mai mult cu cât donatorii mai vârstnici sunt mai puțin tentați să facă donații cash și ar fi tentați în aceeași măsură să privească înregistrările lor ca fiind *„expirate”*. Dar în cazul în care testamentul are o natură contencioasă, organizația non-profit va dori să dovedească că legatorul a fost un susținător loial și va avea nevoie de date/informații ca să facă acest lucru. Într-un scenariu mai tipic este valoros pentru rudele legatorului de a primi o scrisoare în semn de mulțumire pentru generozitatea legatorului. În felul acesta chiar se poate contribui la dezvoltarea unei noi relații cu această generație următoare.

GDPR a început să creeze o schimbare culturală în strângerea de fonduri. Colectorii de fonduri sunt buni la schimbul reciproc de idei și sunt mereu deschiși în a adopta noi modalități de lucru. Cu toate acestea, deseori noile idei sunt pur și simplu transferate de la un organism la altul fără a reflecta prea mult la motivele pentru care o astfel de tactică poate funcționa. GDPR încurajează colectorii de fonduri să creeze o bază de dovezi/mecanisme pentru a justifica de ce folosesc datele cu caracter personal în anumite moduri.

***De exemplu*,** prelucrarea datelor cu caracter personal pentru cercetare poate fi efectuată în interesul legitim al multora dintre organizații, dar ele vor trebui să demonstreze de ce acest lucru este așa. Conformitatea cu GDPR necesită dovezi că cei implicați în acțiuni de cercetare s-ar aștepta în mod rezonabil că o să se întâmple și este puțin probabil să se dorească a se renunța la astfel de activități. Acest lucru este valabil pentru fiecare colector de fonduri în mod individual, dar și pentru întreg sectorul, fiind nevoie ca, sub imperiul GDPR, acțiunile să fie justificate pe bază de dovezi.

Ce este de făcut cu datele donatorilor?

Un domeniu de preocupare acoperit de GDPR este **colectarea de date și stocarea** datelor și cum se aplică aceste reglementări pentru datele cu caracter personal aparținând donatorilor. ONG trebuie să fie capabilă să demonstreze necesitatea colectării și stocării datelor cu caracter personal.

Practica colectării a cât mai multe date personale posibile, din care apoi, în realitate, doar o parte componentă a setului de date sunt prelucrate (restul, în general, nu sunt potrivite pentru atingerea scopului), nu va fi permisă în conformitate cu GDPR.

Capacitatea persoanelor fizice de a formula o solicitare de acces la datele sale și de a cere să vadă datele păstrate despre ei în termenul legal prevăzut de Regulament ar trebui să influențeze decizia ONG de a colecta numai anumite date.

Păstrarea și divulgarea datelor cu caracter personal ale donatorilor

Stocarea ridică alte probleme, pe lângă accesibilitate, precum **securitatea**. Orice tip de date cu caracter personal trebuie să fie stocate în siguranță.

Trebuie să fie instituie măsuri adecvate pentru a vă asigura că datele sunt accesate doar de operator, și nu de către oricine altcineva. Majoritatea incidentelor de securitate apar ca rezultat al erorilor umane, ONG fiind responsabilă pentru instruirea personalului în domeniul securității datelor cu caracter personal.

ONG, de asemenea, trebuie să asigure securitatea end-to-end atunci când datele donatorului sunt transferate către orice furnizor, spre exemplu, agenții de colectare fonduri etc. Nu vă bazați că aceste agenții sunt în conformitate cu regulile GDPR, ci luați-vă dumneavoastră asigurări în acest sens înainte de a semna orice acorduri.

O altă schimbare majoră pe care GDPR o aduce vizează **eliminarea sau ștergerea** datelor cu caracter personal. Majoritatea organizațiilor cu capacitate mare de stocare a datelor personale le dețin pe termen nelimitat. Aceasta se face fie prin stocarea datelor în baza lor de date principală sau ca arhive. Oricum, există riscuri aferente stocării datelor cu caracter personal.

În general, când datele cu caracter personal ale unui donator nu sunt utilizate deoarece nu a mai avut contact cu ONG pentru o perioadă semnificativă de timp este mai bine să le ștergeți, reducând astfel riscurile care pot apărea pentru organizația dumneavoastră.

GDPR impune să stabiliți o perioadă-limită de stocare/arhivare a datelor și, de asemenea, prezentarea unei politici clare pentru ștergerea datelor, eventual în cadrul Politicii de confidențialitate a ONG. Nimeni nu poate stoca datele cu caracter personal pe termen nelimitat, ONG-urile trebuie și au nevoie să fie pro-active atunci când decid ce date cu caracter personal vor păstra și pentru ce perioadă.

În plus, GDPR impune **acuratețea** datelor cu caracter personal. Acesta este sensul comun, datele incorecte valorând puțin, dar poate fi greu să actualizați înregistrările în mod regulat prin audituri. În timp ce poate părea contra-intuitiv este mai bine ca datele care nu mai sunt de actualitate să fie eliminate. În plus, riscul de o încălcare a protecției datelor cu caracter personal prin înregistrări inexacte trebuie să fie atent echilibrat împotriva riscului de a renunța la datele cu caracter personal necesare.

Cum vă asigurați că ați obținut consimțământul donatorului?

Consimțământul este doar una dintre cele șase condiții care vor fi adesea folosite de către organizațiile non-profit **în cazul strângerii de fonduri**. Obținerea consimțământului de a utiliza datele cu caracter personal poate fi totuși o provocare. Sub GDPR, ștacheta a fost ridicată, și de fiecare dată când consimțământul donatorului este solicitat, acesta trebuie să fie lipsit de ambiguitate, demonstrabil, specific și informat.

Este util să vă gândiți că acest consimțământ nu ar trebui să ducă la surprize atunci când datele donatorilor sunt ulterior prelucrate. Luând fiecare cerință în parte:

- Nu va exista nicio confuzie dacă cererea este lipsită de ambiguitate.
- Pentru ca acordul să fie oferit în mod liber, donatorul ar trebui aibă aceeași percepție și să creadă la fel cum o fac cei din organizație. Nu trebuia să dea, dar au ales să facă acest lucru.
- Pentru a fi demonstrabil, consimțământul trebuie să poată fi demonstrat; când și cum a fost acordat consimțământul. Obținerea consimțământului prin telefon poate fi greu de demonstrat și necesită excelență în procesul următor, mai exact în înregistrarea a ceea ce s-a spus.

Următoarele două cerințe vor ridica provocări mai mari pentru organizațiile non-profit:

- Consimțământul specific înseamnă că: Donatorii trebuie să aibă posibilitatea de a alege și aceste opțiuni trebuie să fie reale și granulare. Unii oameni vor să facă asta, aud despre activitățile ONG, dar nu doresc să le fie ceruți bani. Fondatorii vor trebui să facă acest lucru, să se folosească de abilitățile lor în a cere bani și atunci când cer oamenii să furnizeze datele lor pentru a putea fi contactați/întrebați în viitor.
- Această granularitate face să fie importantă informarea persoanelor vizate despre ce înseamnă consimțământul lor. Organizațiile non-profit vor trebui să fie mai deschise despre planurile lor de strângere a fondurilor și mai pregătite pentru consecințele care se pot ivi.

Interpretarea justă a GDPR

Scopul GDPR este de a autoriza persoanele vizate și de a proteja drepturile acestora.

Corectitudinea înseamnă că organizațiile trebuie să fie absolut transparente în legătură cu următoarele aspecte:

- De ce colectează datele cu caracter personal (spre exemplu ale donatorilor)?

- Ce fac cu datele personale colectate?
- Cu cine împărtășesc datele cu caracter personal ale donatorilor?
- Cum stochează datele cu caracter personal?
- Cât timp păstrează datele cu caracter personal?
- Când pot avea acces persoanele vizate la datele lor cu caracter personal?

Datele cu caracter personal sunt înțelese ca un bun pe care o organizație, cum ar fi o organizație non-profit, le colectează și le utilizează. Expresii cum ar fi „date miniere” (adică transformarea datelor primare în informații utile; terminat prin utilizarea de software pentru a căuta modele în loturi mari de date) reflectă atitudinea față de datele agregate. Dar fiecare strat dintr-o mină de date ar putea fi datele personale ale unui individ.
GDPR pune controlul înapoi în mâinile persoanei vizate. Ele pot da datele lor cu caracter personal mai departe pentru a fi prelucrate, dar datele sunt doar „împrumutate” și operatorul de date are responsabilitatea de le trata cu mare grijă.

GDPR cere organizațiilor să se asigure că au politicile și procedurile corecte și eficiente înainte de a face orice încercări de a colecta sau a prelucra date cu caracter personal. Politicile trebuie să se asigure că există organizații non-profit mai transparente în prelucrarea datelor cu caracter personal și să comunice mai eficient cu persoanele vizate. În plus, GDPR se asigură că organizațiile au capacitatea și raționamentul justificat pentru colectarea și stocarea datelor cu caracter personal. Aceasta înseamnă că datele ar trebui să fie colectate doar dacă există o legitimitate pentru a se folosi de ele. Fără a avea mijloace adecvate de colectare, stocare, actualizare și ștergere, organizațiile vor încălca GDPR.

În cele din urmă, GDPR solicită organizațiilor nu numai să fie conforme cu Regulamentul, ci și să monitorizeze și să testeze această conformitate. Dacă există încălcări de date, atunci există cerințe stricte de raportare a încălcării către ANSPDCP în termen de 72 de ore. O încălcare a datelor cu caracter personal privind strângerea de fonduri ar trebui, de asemenea, să fie raportată către board-ul ONG ca fiind un incident grav.

Colectorii de fonduri – terțe părți

Organizațiile non-profit care lucrează cu organizații de strângere de fonduri de la terți, inclusiv consultanți, fondatori, agenții și furnizori independenți, trebuie să se asigure că furnizorul terț respectă aceleași standarde ca și organizația non-profit.

Aceasta înseamnă că organizațiile TREBUIE să solicite oricărei terțe părți sau unei agenții să respecte cerințele din cadrul GDPR și din reglementările speciale în materie, indiferent de jurisdicția țării sau jurisdicției în care agenția își are sediul sau funcționează.

Organizațiile trebuie să realizeze o monitorizare eficientă și proporțională a oricăror contracte încheiate cu terțe părți. Organizațiile non-profit ar trebui, de asemenea, să se asigure că donatorii știu unde și cum pot raporta toate neregulile și presupusele încălcări care rezultă din practicile de strângere de fonduri ale unor terțe părți.

Examinarea riscurilor modelelor de afaceri ale organizațiilor non-profit

GDPR încearcă să promoveze o cultură de conștientizare a riscurilor la nivelul organizațiilor care gestionează orice tip de date cu caracter personal. De asemenea, acordă importanță și valoare informării persoanelor vizate cu privire la drepturile lor.

Riscul pe care GDPR îl prezintă modelelor de afaceri ale organizațiilor non-profit este destul de însemnat. Dacă organizațiile non-profit reușesc să se conformeze GDPR și nu există încălcări ale datelor raportate pe scară largă, încrederea în acest sector va fi probabil ridicată. Cu toate acestea, dacă există o percepție conform căreia organizațiile non-profit nu respectă drepturile subiecților donatori, atunci acestea ar putea avea un impact negativ asupra activităților de strângere de fonduri și ar putea reduce venitul general.

Accentul pus pe atingerea conformității cu GDPR a evidențiat faptul că numeroase organizații non-profit începuseră să devină neconforme cu cerințele lor în conformitate cu legislația anterioară în domeniul protecției datelor cu caracter personal.

Ar trebui să vă faceți timp pentru a rezolva aceste probleme și pentru a pune în aplicare politici în conformitate cu noile cerințe legislative. Acest lucru presupune ca organizațiile să-și folosească timpul, resursele umane și financiare, să identifice domeniile de îngrijorare și să rezolve imediat problemele.

Modelele de afaceri ale ONG se dezvoltă adesea de-a lungul anilor de practică și poate fi dificil să se schimbe comportamentul organizațional într-un interval de timp limitat pentru a promova bunele practici.

Riscul unei încălcări a datelor pentru o organizație non-profit poate fi redus, însă consecința unei amenzi de 20 de milioane de euro sau 4% din cifra de afaceri globală, luându-se în considerare cea mai mare valoare, înseamnă că ar trebui să influențeze modelul de afaceri al fiecărui organism. Evitarea acestui risc poate fi atenuată prin numirea unui responsabil cu protecția datelor cu caracter personal (DPO), care va fi capabil să rămână la curent cu viitoarele tendințe și modificări ale GDPR. Multe organizații non-profit desemnează DPO externi, în special în cazul în care taxele includ o indemnizație împotriva riscului de amendă ca urmare a consultării DPO-ului.

De asemenea, riscul poate fi evitat printr-un program cuprinzător și continuu de formare a personalului cu privire la utilizarea datelor cu caracter personal în cadrul GDPR. Majoritatea încălcărilor apar din cauza erorilor umane, astfel încât lucrul cu personalul și cu voluntarii este cel mai important aspect de la care merită să începeți atunci când vine vorba de reducerea acestei probabilități.

2.3. Managementul datelor financiare și GDPR

Organizațiile non-profit trebuie să evalueze procesele lor financiare de natură a asigura respectarea cerințelor GDPR, identificarea oricăror deficiențe și construirea unor noi procese pentru a fi în conformitate cu GDPR.

Recomandăm construirea și punerea în aplicare de către o echipă special formată a unui program GDPR în sensul de a efectua analize, a răspunde nevoilor GDPR și tranziției către GDPR.

GDPR obligă organizațiile non-profit să se asigure că procesele lor financiare sunt conforme cu principiile GDPR:

- conformarea cu dispozițiile GDPR și demonstrarea conformității – principiul responsabilității;
- asigurarea că a fost identificat prealabil prelucrării un temei legal pentru prelucrarea datelor cu caracter personal;
- oferirea persoanelor vizate informații despre ce se întâmplă cu datele lor, inclusiv copiilor cărora trebuie ca aceste informații să fie acordate într-un format ușor de citit;
- instituirea unui sistem care să permită părinților furnizarea consimțământului pentru copilul care nu a împlinit vârsta minimă legală;
- încheierea de acorduri/contracte cu orice organizație care prelucrează date cu caracter personal în numele ONG, care să fie actualizate cu clauze supuse monitorizării.

Trebuie să redactați politici și proceduri care să documenteze orice proces care implică date financiare, date care ar trebui să fie clasificate ca informații cu caracter personal. O provocare-cheie pentru multe organizații este de a fi capabile să înțeleagă ce date cu caracter personal deține și să le fie clar cum sunt prelucrate și partajate în cadrul ONG și cu terții.

În general, există o nevoie clară să înțelegeți ce date personale financiare dețineți, atât în înregistrările fizice, cât și în cele electronice. Acest lucru poate necesita realizarea unui audit al datelor cu caracter personal acoperind toate înregistrările (fără a se limita la):

- înregistrări ale angajaților, incluzând salariul, cereri de creditare, înregistrări aferente pensiilor;
- înregistrările voluntarilor, incluzând detalii financiare personale și cheltuieli;
- susținători și date aferente strângerilor de fonduri, inclusiv donațiile sau alte ajutoare financiare;
- informații ale furnizorilor, inclusiv adresa de e-mail sau informațiile de contact ale celor care vă furnizează bunuri sau servicii;
- date financiare aferente beneficiarilor, subvenții, analize financiare pentru acordarea unor burse și/sau înregistrări salariale.

Auditarea datelor cu caracter personal este un pas important în înțelegerea și cunoașterea datelor pe care le dețineți, unde se află și care este baza legală în temeiul căruia au fost obținute.

În plus, trebuie să stabiliți clar partajarea responsabilității între operatorul de date și persoana împuternicită, și trebuie să fiți sigur că dacă orice terțe părți dețin aceste date în numele dumneavoastră, cum ar fi un furnizor de salarizare sau pensii, acestora din urmă le sunt clare responsabilitățile lor. Un audit al datelor cu caracter personal ar putea să parcurgă mai multe medii, inclusiv:

- prezentări introductive personalului-cheie;
- chestionare trimise tuturor unităților de afaceri/unităților operaționale pentru a capta datele cu caracter personal pe care le dețin;
- luarea în considerare dacă toate datele financiare deținute rămân relevante pentru scopul pentru care au fost obținute;
- cum au fost stocate și eliminate înregistrările.

Acest lucru trebuie să fie susținut de o politică clară și ușor de înțeles și de un anumit cadru procedural – acest lucru ar trebui stabilit în funcție de baza legală utilizată pentru colectarea datelor cu caracter personal, pentru ce anume sunt utilizate datele și cât timp

trebuie să fie stocate, aspecte care trebuie să fie comunicate tuturor persoanelor împuternicite de operator – ONG sau terță parte.

Raportarea datelor financiare

Cerințele în ceea ce privește raportarea datelor financiare (sub imperiul GDPR) sunt, în general, în conformitate cu reglementarea anterioară.

În general, majoritatea rapoartelor financiare încheiate pentru o distribuție mai largă sunt fie anonimizate (de exemplu, raportarea cheltuielilor cu salarizarea) sau au un anumit grad de pseudonimizare aplicat (în cazul în care înregistrările angajaților sunt menționate într-un raport, dar acestea nu conțin nume/adrese) și, ca atare, ar necesita informații suplimentare pentru a identifica persoanele implicate.

Diferențele-cheie sunt date de tipurile de raportări pentru care se listează date personale financiare – în timp ce procedurile sunt instituite pentru a gestiona securitatea datelor, sub imperiul GDPR există termene de raportare a încălcărilor de securitate și un risc mai mare pentru potențiale amenzi. Ca atare, ar trebui să fie considerată o bună practică cunoașterea persoanei responsabile să genereze astfel de rapoarte care să fie capabilă să urmărească producția, diseminarea și eliminarea lor când nu mai sunt necesare.

Cadrul procedural și politicile, de asemenea, ar trebui să fie clare în acest domeniu – în cazul în care datele sunt prelucrate ca o parte dintre scopurile legitime ale organizației, acest lucru ar trebui să fie clar, astfel încât, în cazul în care există orice cereri în respectarea „dreptului de a fi uitat”, acestea să poată fi refuzate sau prelucrate eficient.

Eliminarea datelor financiare

Eliminarea datelor financiare ar trebui să fie în concordanță cu politica redactată și instituită în acest sens, recunoscând perioade de reținere legale. Odată eliminate, trebuie să existe asigurări că procesul de eliminare a fost sigur și monitorizat pentru ca datele să nu fie pierdute și să nu ajungă la o terță parte.

2.4. Datele cu caracter personal ale Beneficiarilor și GDPR

Protejați-vă datele cu caracter personal și beneficiarii

Este foarte important să înțelegeți care sunt datele cu caracter personal pe care le dețineți pentru beneficiari, incluzând orice format, fizic/electronic. Recomandăm să efectuați un audit asupra tuturor înregistrărilor ce conțin date cu caracter personal, inclusiv (dar nu limitat la):

- Înregistrările despre beneficiari, inclusiv perioada de timp pentru care le veți păstra
- Locația și tipurile de înregistrări deținute și care a fost munca întreprinsă pentru obținerea și curățarea lor
- Claritate cu privire la ceea ce conțin înregistrările – date sensibile, inclusiv date referitoare la copii și afecțiuni medicale
- Procesele prin care s-au obținut datele beneficiarilor și unde sunt ținute, inclusiv dacă există o dublură între înregistrări manuale/electronice
- Date financiare ale beneficiarilor, cum ar fi ajutoarele financiare, analize și/sau înregistrări salariale
- Țările terțe către care datele pot fi transferate
- Persoanele responsabile pentru protecția datelor în fiecare stadiu al prelucrării.

Efectuarea unui audit este un pas important în înțelegerea și cunoașterea datelor cu caracter personal pe care le dețineți, unde se află și care este baza legală în temeiul căreia au fost obținute.

În plus, trebuie să stabiliți în mod clar care este responsabilitatea operatorului de date și care este responsabilitatea persoanei împuternicite, și dacă orice terțe părți dețin aceste date în numele dumneavoastră, cum ar fi un furnizor de salarizare sau pensii, acestora din urmă le sunt clare responsabilitățile lor. Un audit al datelor cu caracter personal ar putea să parcurgă mai multe medii, inclusiv:

- Prezentări introductive personalului-cheie

- Chestionare trimise tuturor unităților de afaceri/unităților operaționale pentru a capta datele cu caracter personal pe care le dețin
- Luarea în considerare dacă toate datele financiare deținute rămân relevante pentru scopul pentru care au fost obținute
- Cum au fost stocate și eliminate înregistrările.

Acest lucru trebuie să fie susținut de o politică clară și ușor de înțeles și de un anumit cadru procedural – acest lucru ar trebui stabilit în funcție de baza legală utilizată pentru colectarea datelor cu caracter personal, pentru ce anume sunt utilizate datele și cât timp trebuie să fie stocate, aspecte care trebuie să fie comunicate tuturor persoanelor împuternicite de operator – ONG sau terță parte.

GDPR impune organizațiilor să comunice persoanelor vizate informații suplimentare. ***Spre exemplu*****,** baza legală de prelucrare, perioada de stocare a datelor și dreptul de a se plânge către ANSPDCP. Va trebui, de asemenea, să vă pregătiți pentru a răspunde cererilor de acces formulate de persoanele vizate. Printre acțiunile preparatorii indicăm:

- proiectați un șablon de răspuns, astfel încât să vă puteți asigura că sunt respectate toate cerințele prevăzute de Regulament;
- dezvoltați politici și proceduri pentru gestionarea cererilor de acces și pentru asigurarea respectării termenului legal;
- asigurați-vă că angajații sunt instruiți în privința gestionării cererilor de acces, aceștia fiind capabili să recunoască o astfel de cerere și cum va trebui să o abordeze.

Luați în considerare următoarele aspecte:

- ✓ Rețineți vreo dată cu caracter personal care nu mai este relevantă (cu excepția perioadelor pentru care legea vă autorizează să le dețineți, spre exemplu, pentru plata impozitelor și taxelor)?
- ✓ Suplimentar, dacă unele dintre datele deținute au suferit modificări, ar trebui reconsiderată prioritizarea înregistrărilor necesar a fi deținute în continuare.

- ✓ ONG ar trebui să clarifice în cadrul contractelor cu privire la datele cu caracter personal aparținând beneficiarilor, scopul prelucrării, durata și motivele dezvăluirii/divulgării.
- ✓ Dacă datele cu caracter personal vor fi folosite pentru un alt scop, cum ar fi cercetarea sau evaluarea performanțelor ONG-ului în realizarea unui proiect, ca parte a unei evaluări de ansamblu, recomandăm ca aceste date să fie anonimizate.
- ✓ Dacă prelucrați date cu caracter personal speciale luați în considerare efectuarea unei evaluări de impact cu privire la protecția datelor cu caracter personal (DPIA).

În ansamblu, ONG trebuie să fie transparentă în privința datelor cu caracter personal obținute și prelucrate în funcție de diferite temeiuri legale de prelucrare – aspecte care trebuie să fie clare și beneficiarilor. De asemenea, aceste aspecte trebuie să fie clare personalului și voluntarilor.

Pentru datele beneficiarilor, prelucrarea ar putea să aibă loc în temeiul consimțământului, în temeiul unui contract, interesului legitim sau interes vital.

Consimțământul poate că nu este necesar întotdeauna pentru prelucrarea datelor cu caracter personal aparținând beneficiarului. În multe situații, prelucrarea poate avea loc în temeiul interesului legitim.

Spre exemplu, dacă datele beneficiarului au fost obținute sub imperiul interesului legitim, acest lucru ar trebui evidențiat și comunicat beneficiarului. Din perspectiva ONG există o nevoie de a demonstra finanțatorilor munca care a fost realizată, furnizându-le un audit al muncii lor pentru validare. În orice caz, dacă datele beneficiarului sunt utilizate pentru orice alt scop decât cel pentru care au fost colectate (spre exemplu, în materiale de marketing), consimțământul ar trebui obținut.

GDPR introduce reguli speciale pentru protecția datelor cu caracter personal aparținând copiilor în special în contextul serviciilor informaționale. Organizațiile care oferă servicii online pentru copii și se bazează pe consimțământ pentru a colecta informații vor fi direct

afectate și trebuie să se asigure că limbajul utilizat este adaptat pentru publicul-țintă. Prelucrarea datelor referitoare la copii este evidențiată cu anumite riscuri și implicit, cu anumite restricții. Sub imperiul art. 8 alin. (2) din Regulament, organizațiile non-profit trebuie să depună eforturi rezonabile pentru a verifica dacă consimțământul a fost acordat sau autorizat de persoana în drept (părinte/tutore etc.). În orice caz, organizațiile non-profit vor putea prelucra date cu caracter personal dacă prelucrarea se referă la servicii de prevenție și consiliere oferite în mod direct unui copil și fără a verifica calitatea persoanei căreia consimțământul îi aparține.

Dacă baza legală de prelucrare este interesul legitim va trebui să documentați acest aspect și eventual să efectuați o DPIA dacă prelucrarea privește date cu caracter personal aparținând copiilor. De asemenea, recomandăm efectuarea unei DPIA și atunci când prelucrarea are ca obiect informații sensibile despre beneficiari, spre exemplu, informații medicale, despre condamnări sau alte asemenea informații, situație în care trebuie să întocmiți proceduri clare de contactare a beneficiarilor.

Important! În cazul în care organizația desfășoară activități în mai mult de un stat membru al UE (adică efectuează prelucrări transfrontaliere) ar trebui să stabiliți autoritatea de supraveghere principală. În acest sens, organizația va trebui să își mapeze locurile în care se iau deciziile semnificative și cu impact cu privire la prelucrările de date cu caracter personal. De asemenea, ar trebui să luați în considerare dacă datele vor fi transferate în afara UE – situație în care sunteți obligat să solicitați clarificări de la partea terță care prelucrează datele pentru dumneavoastră, să cunoașteți garanțiile instituite în raport de țara terță și când va trebui să obțineți consimțământul pentru prelucrarea datelor cu caracter personal în afara UE.

Raportarea datelor cu caracter personal ale beneficiarilor

În general, majoritatea înregistrărilor cu o distribuție mai largă ar trebui să fie anonimizate (de exemplu, rapoartele de cercetare) sau să aibă instituite un anumit grad de pseudonimizare (în cazul în care înregistrările nu conțin nume/adresă) și, ca atare, ar fi nevoie de informații suplimentare în vederea stabilirii persoanelor implicate.

Notă: Aspectele menționate la punctul anterior *„Raportarea datelor financiare”* își au aplicabilitatea și în cazul datelor cu caracter personal aparținând beneficiarilor.

Eliminarea datelor cu caracter personal aparținând beneficiarilor

Eliminarea datelor aparținând beneficiarilor ar trebui să fie în concordanță cu politica redactată și instituită în acest sens, recunoscând perioade de reținere legale. Odată eliminate, trebuie să existe asigurări că procesul de eliminare a fost sigur și monitorizat astfel încât datele cu caracter personal să nu fie pierdute sau să ajungă la o terță parte neîndreptățită să ia la cunoștință de ele.

2.5. Datele cu caracter personal ale angajaților și GDPR

Înțelegerea responsabilității ca angajator

Organizațiile non-profit nu trebuie doar să se conformeze cu cerințele și principiile GDPR, ci ele trebuie în aceeași măsură să poată dovedi conformitatea și responsabilitatea lor.

Acest lucru necesită revizuirea a:

- ✓ datelor cu caracter personal ale angajaților și voluntarilor pe care le deținеți și le prelucrați;
- ✓ cum sunt aceste date cu caracter personal utilizate;
- ✓ care este baza legală pentru prelucrarea datelor cu caracter personal aparținând angajaților și voluntarilor.

Va trebui, de asemenea, să creați loguri cu datele deținute și prelucrate și să le puneți la dispoziția ANSPDCP la cerere în cazul unei inspecții.

Va trebui să identificați pe cineva care va avea responsabilitatea pentru asigurarea conformității curente cu GDPR. Dacă această persoană este responsabilul cu protecția datelor, acest lucru va depinde de mărimea organizației și cantitatea de date cu caracter personal prelucrate.

Ar trebui ca un ONG să depindă de consimțământul explicit al angajaților săi pentru prelucrarea datelor cu caracter personal? Răspunsul este negativ. ONG poate prelucra datele cu caracter personal ale angajaților în temeiul art. 6 alin. (1) lit. b) – prelucrarea este necesară pentru încheierea/executarea unui contract la care persoana vizată este parte.

Important: Nu este conform cu GDPR introducerea unei clauze în contract formulate în sensul *„prin semnarea prezentului contract, persoana vizată consimte la prelucrarea datelor cu caracter personal”.*

Un alt domeniu-cheie pe care organizațiile non-profit vor trebui să îl aibă în vedere și să îl revizuiască este **formarea angajaților și voluntarilor** privind protecția datelor cu caracter personal în scopul de a vă asigura că aceștia sunt conștienți de responsabilitatea crescută a organizației pentru prelucrările de date cu caracter personal și, implicit, în privința posibilelor sancțiuni.

Cum schimbă GDPR modul în care organizațiile non-profit dețin și prelucrează datele cu caracter personal aparținând angajaților?

Organizațiile non-profit, la fel ca orice altă organizație, obțin și rețin date cu caracter personal printr-o varietate de moduri, precum: date aferente dosarului personal, forme contractuale, beneficii ale aplicațiilor, comunicări prin e-mail, înregistrări electronice etc.

Sub imperiul principalelor principii ale GDPR, datele cu caracter personal trebuie să fie colectate în scopuri specifice, prelucrate în mod legal, datele trebuie să fie actualizate și exacte și trebuie să fie reținute într-o formă care să permită identificarea persoanei vizate pentru nu mai mult decât este necesar. Organizațiile non-profit vor trebui să revizuiască datele stocate în mod curent despre angajați și voluntari și să aprecieze dacă acestea rămân relevante sau pot fi șterse sau anonimizate.

Până în prezent, organizațiile non-profit nu aveau nicio responsabilitate pentru vreo parte terță (spre exemplu, agenție de recrutare) referitor la prelucrările de date sau în furnizarea datelor cu caracter personal. Sub imperiul GDPR, acest lucru înseamnă că organizațiile non-profit vor trebui să se asigure că orice parte terță la care transmite datele personale este compliant cu GDPR. Va trebui astfel să existe o atenție sporită în alegerea persoanei împuternicite sau furnizorului și va trebui să se încheie acorduri/contracte pentru repartizarea responsabilității pentru conformitatea cu GDPR.

Ce trebuie să facă ONG cu datele aparținând angajaților?

Datele angajaților trebuie să fie stocate în siguranță și pentru perioada pentru care sunt necesare indiferent de formatul în care se află. Organizațiile vor trebui să revizuiască procesele/operațiunile curente și să se asigure că datele angajaților sunt revizuite din perspectiva relevanței în funcție de o anumită bază legală. Adesea există obligații legale care impun păstrarea datelor personale pentru o anumită perioadă de timp sau de a păstra înregistrări care să vă permită să vă apărați împotriva acțiunilor în justiție formulate.

Pentru o analiză detaliată referitoare la aplicarea Regulamentului în **privința angajaților** vă recomandăm să cercetați lucrarea **Protecția Datelor cu Caracter Personal – Ghid pentru HR.**

Cum trebuie să procedați cu voluntarii?

Organizațiile non-profit adesea lucrează cu voluntari, prelucrând implicit datele cu caracter personal care le aparțin.

Așa cum ONG trebuie să procedeze cu datele personale ale angajaților, în aceeași măsură trebuie să aplice cerințele GDPR și față de datele cu caracter personal aparținând voluntarilor. La fel ca în cazul angajaților, organizațiile trebuie să comunice cu voluntarii săi în ceea ce privește datele cu caracter personal pe care le dețin, le prelucrează, pentru ce perioadă și cum sunt eliminate. Astfel că, dacă aveți voluntari ale căror date le prelucrați, trebuie să asigurați aceleași standarde de protecție și transparență similare angajaților (în special atunci când voluntarii se ocupă de servicii de livrare și suport).

Voluntarii pot continua să fie persoane vizate pentru o organizație și implicit să fie supuși regulilor cu privire la protecția datelor cu caracter personal chiar și după ce relația a încetat. Organizațiile ar trebui să își ia măsuri suplimentare de precauție atunci când voluntarii sunt esențiali pentru serviciile de livrare și pot fi responsabili pentru datele cu

caracter personal speciale/sensibile. Un angajament contractual ar fi o modalitate ideală de a stabili responsabilitatea voluntarilor care prelucrează date cu caracter personal. De asemenea, ar trebui să fie stabilită necesitatea efectuării unei instruiri a acestora, precum și procedura de raportare a incidentelor de securitate.

3. Relația operator – persoană împuternicită de operator

CUI divulgați datele cu caracter personal?

Operator de date cu caracter personal: ONG

Împuterniciți/Operatori asociați:

- ✓ Autorități/Instituții publice
- ✓ Programatori
- ✓ Firme de contabilitate
- ✓ Entități bancare
- ✓ CRM
- ✓ Furnizori de marketing (integrali sau specializați – de ex. Newsletter – Mailchimp etc.)
- ✓ Terți care sunt integrați în website – Google Analytics, Facebook Like etc.

3.1. Contractul dintre operator și persoana împuternicită

Contractul încheiat între operator și persoana împuternicită trebuie să includă în mod obligatoriu următoarele aspecte:

- Obiectul și durata prelucrării
- Natura și scopul prelucrării
- Tipul de date cu caracter personal și categoriile de persoane vizate și
- Obligațiile și drepturile operatorului de date.

Contractul încheiat între operator și persoana împuternicită trebuie să includă următoarele **clauze obligatorii**:

- Persoana împuternicită trebuie să acționeze numai pe baza instrucțiunilor operatorului *(cu excepția cazului în care legea o obligă să acționeze în lipsa unor instrucțiuni).*
- Persoana împuternicită trebuie să se asigure că personalul care se ocupă de prelucrarea datelor respectă confidențialitatea *(ex: prin încheierea unei clauze de confidențialitate sau includerea unei astfel de clauze în statutul persoanei împuternicite)*.
- Persoana împuternicită trebuie să ia măsurile corespunzătoare pentru a asigura securitatea prelucrării.
- Persoana împuternicită are permisiunea de a angaja un sub-contractant persoană împuternicită cu acordul prealabil al operatorului și în baza unui contract scris.
- Persoana împuternicită trebuie să asiste operatorul de date în furnizarea accesului persoanelor vizate la datele lor, precum și să permită persoanelor interesate să-și exercite drepturile lor în conformitate RGPD.
- Persoana împuternicită trebuie să asiste operatorul de date în îndeplinirea obligațiilor sale potrivit RGPD în legătură cu securitatea prelucrării, notificarea încălcărilor și evaluările de impact.
- Persoana împuternicită trebuie să șteargă sau să predea toate datele personale operatorului, așa cum a solicitat la încheierea contractului.

- Persoana împuternicită trebuie să prezinte audituri și inspecții, și să furnizeze operatorului orice informații are nevoie pentru a se asigura că atât el, în calitate de operator, cât și persoana împuternicită îndeplinesc obligațiile din articolul 28 RGPD, și trebuie să anunțe imediat operatorul dacă se vede pus în situația de a face ceva ce încalcă RGPD sau alte reglementări în materie.

Ca o chestiune de bună practică, contractele:

- trebuie să prevadă că nicio clauză contractuală nu poate deroga de la prevederile legale ce stabilesc răspunderea persoanei împuternicite conform RGPD; și
- reflectă orice indemnizație convenită.

Responsabilitățile persoanei împuternicite. Limite

În plus față de articolul 28 alin. (3) din Regulament privind obligațiile contractuale, persoana împuternicită are următoarele **atribuții directe** sub imperiul RGPD. Persoana împuternicită trebuie să:

- acționeze numai în baza instrucțiunilor operatorului (articolul 29);
- nu apeleze la un sub-contractant persoană împuternicită fără autorizarea prealabilă scrisă a operatorului (articolul 28 alin. (2));
- coopereze cu autoritățile de supraveghere, în conformitate cu articolul 31;
- asigure securitatea prelucrărilor sale, în conformitate cu articolul 32;
- țină o evidență a activităților sale de prelucrare, în conformitate cu articolul 30 alin. (2) RGPD;
- notifice orice încălcări de date cu caracter personal operatorului, în conformitate cu articolul 33 RGPD;
- angajeze un responsabil cu protecția datelor dacă este necesar, în conformitate cu articolul 37 RGPD; și
- în cazul în care sediul persoanei împuternicite nu se află pe teritoriul UE, obligația de a numi (în scris) un reprezentant în cadrul Uniunii Europene.

O persoană împuternicită, de asemenea, ar trebui să fie conștientă de faptul că:

- ✓ ar putea fi supuse investigațiilor și măsurilor corective care intră în competența autorităților de supraveghere, în temeiul articolului 58 din RGPD;
- ✓ în cazul în care nu reușește să îndeplinească obligațiile sale, poate fi supusă unei amenzi administrative, în conformitate cu articolul 83 din RGPD;
- ✓ în cazul în care nu reușește să își îndeplinească obligațiile, poate fi supusă unei sancțiuni diferite stabilite prin reglementările naționale, în conformitate cu articolul 84 din RGPD; și
- ✓ în cazul în care nu reușește să își îndeplinească obligațiile sale ar putea fi obligată să plătească despăgubiri către persoana vizată păgubită, în conformitate cu articolul 82 din RGPD.

3.2. Clauze pentru contractele cu împuterniciți

** furnizorii de aplicații informatice și soluții tehnice care sunt împuterniciți de operator să realizeze operațiunile tehnice prin care se efectuează (o parte) din prelucrarea datelor cu caracter personal necesară pentru desfășurarea activității CLIENT.*

I. Împuternicitul [...] realizează pentru CLIENT următoarele activități de prelucrare a datelor cu caracter personal: [...lista integrală a tipurilor de date personale, operațiunilor de prelucrare, natura și obiectul lor, cu menționarea categoriilor de persoane vizate...].

Scopul prelucrării realizate de [...] pentru CLIENT este: [...].

Durata prelucrării realizate de [...] pentru CLIENT este: [...].

II. Potrivit dispozițiilor art. 28 alin. (1) Regulamentului (UE) 2016/679, împuternicitul oferă CLIENTULUI garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte cerințele prevăzute în prezentul regulament și să asigure protecția drepturilor persoanei vizate, după cum urmează: [...].

III. CLIENT va putea realiza verificarea garanțiilor organizatorice și tehnice invocate de împuternicit în orice moment. Garanțiile insuficiente sau, după caz, împiedicarea în orice formă a verificării lor, justifică rezilierea imediată a contractului dintre părți, cu daune interese pentru îngreuierea activității CLIENT.

IV. Pentru îndeplinirea obligațiilor sale contractuale, persoana împuternicită nu va recruta o altă persoană împuternicită fără autorizație scrisă prealabilă din partea CLIENT.

V. Modalitățile tehnice și soluțiile de conservare a evidenței prelucrărilor de date cu caracter personal pentru CLIENT sunt următoarele: [...]

VI. Modalitățile tehnice și organizatorice prin care persoana împuternicită [...] îl asigură pe operator că orice persoană fizică care acționează sub autoritatea sa și care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului CLIENT sunt: [...]

VII. Persoana împuternicită de operator înștiințează operatorul neîntârziat cu privire la orice încălcare a securității datelor cu caracter personal. Notificarea va cuprinde cel puțin elementele prevăzute de art. 33 alin. (3) din Regulamentului (UE) 2016/679.

VIII. Prevederile din contract care atrag incidența unor clauze penale sunt următoarele: [...]

IX. Cheltuielile de conformare cu dispozițiile Regulamentul (UE) 2016/679, cheltuielile de adaptare, cheltuielile de raportare, autorizare și informare vor fi suportate astfel: [...]

X. Orice comunicare cu privire la prezentul contract se va face utilizând următoarele canale: [...]

XI. Persoanele desemnate pentru comunicare între părți în legătură cu prezentul contract sunt: [...].

3.3. Clauze pentru contractul cu operatorii asociați

** aceste clauze trebuie negociate foarte atent, întrucât, deși ele transpun obligații izvorâte din dispozițiile imperative ale GDPR, vor stârni o puternică rezistență din partea operatorilor asociați, întrucât obligațiile lor sunt mai împovărătoare decât cele prevăzute de GDPR în raport cu datele cu caracter personal ale persoanelor vizate pe care le colectează ei înșiși în mod direct.*

I. CLIENT și [...] stabilesc în comun scopurile și mijloacele de prelucrare a datelor cu caracter personal ale persoanelor vizate, în conformitate cu obligațiile care le revin potrivit Regulamentului (UE) 2016/679.

II. În scopul informării persoanelor vizate de către CLIENT, operatorul asociat [...] declară și, respectiv, recunoaște cu caracter de obligații:
1. identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia: [...]
2. datele de contact ale responsabilului cu protecția datelor, după caz: [...]
3. scopurile în care operatorul asociat sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării: [...]
4. în cazul în care 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, descrierea scopurilor legitime: [...]
5. destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
6. dacă este cazul, intenția operatorului asociat [...] de a transfera date cu caracter personal către o țară terță sau o organizație internațională și existența sau absența unei decizii a Comisiei privind caracterul adecvat, sau garanții adecvate prin clauze contractuale propuse de operatorul asociat [...], aprobate de CLIENT și autorizate de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal cf. art. 46 alin. (3) lit. (a) din Regulamentul (UE) 2016/679.

III. Având în vedere cerința ca CLIENT să furnizeze persoanelor vizate informații suplimentare necesare pentru a asigura o prelucrare echitabilă și transparentă a datelor cu caracter personal, operatorul asociat [...] declară și, respectiv, recunoaște cu caracter de obligații:

1. perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă: [...]

2. existența obligației operatorului asociat în ceea ce privește datele cu caracter personal referitoare la persoanele vizate ca, la solicitarea directă a acestora sau la solicitarea CLIENT, să permită accesul la datele cu caracter personal, rectificarea sau ștergerea acestora, să restricționeze sau să oprească prelucrarea, precum și obligațiile corelative dreptului la portabilitatea datelor;

3. că atunci când prelucrarea se bazează pe consimțământul explicit al persoanei vizate pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice, persoana vizată are dreptul de a-și retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;

4. 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: [...]

5. dacă este cazul, existența unui proces decizional automatizat incluzând crearea de profiluri, precum și informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoanele vizate: [...]

IV. În cazul în care operatorul asociat [...] intenționează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, informații privind scopul secundar respectiv și orice informații suplimentare relevante: [...]

V. Esența acordului dintre CLIENT și operatorul asociat [...] care va fi adusă la cunoștința persoanelor vizate cf. art. 26 alin. (2) din Regulamentul (UE) 2016/679 este formulată după cum urmează: [...]

VI. Cheltuielile de conformare cu dispozițiile Regulamentul (UE) 2016/679, cheltuielile de adaptare, cheltuielile de raportare, autorizare și informare vor fi suportate astfel: [...]

VII. Orice comunicare cu privire la prezentul contract se va face utilizând următoarele canale: [...]

VIII. Persoanele desemnate pentru comunicare între părți în legătură cu prezentul contract sunt: [...].

IV. Drepturile persoanelor vizate în ceea ce privește activitatea cabinetelor ONG-urilor

În procedurile operatorului privind prelucrarea datelor cu caracter personal trebuie să fie prevăzute modalități de facilitare a exercitării de către persoana vizată a drepturilor care îi sunt conferite prin GDPR, inclusiv mecanismele prin care aceasta poate solicita și, dacă este cazul, obține, în mod gratuit, în special, acces la datele cu caracter personal, precum și rectificarea sau ștergerea acestora, și exercitarea dreptului la opoziție.

ONG-ul ar trebui să ofere, de asemenea, modalități de introducere a cererilor pe cale electronică, mai ales în cazul în care datele cu caracter personal sunt prelucrate prin mijloace electronice, cum este cazul aplicărilor pentru un job prin intermediul unei platforme online. De asemenea, ar trebui să aibă obligația de a răspunde cererilor persoanelor vizate fără întârzieri nejustificate și cel târziu în termen de o lună și, în cazul în care nu intenționează să se conformeze respectivele cereri, să motiveze acest refuz.

1. Dreptul de acces

Dreptul de acces al persoanei vizate presupune ca aceasta să obțină din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc. În caz afirmativ, trebuie să aibă acces la următoarele informații:

- scopurile prelucrării;
- categoriile de date cu caracter personal vizate;
- 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;
- 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;

- 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;
- dreptul de a depune o plângere în fața Autorității de Supraveghere;
- în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informații disponibile privind sursa acestora;
- existența unui proces decizional automatizat incluzând crearea de profiluri, precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

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.

2. Dreptul la rectificarea datelor

Dreptul la rectificarea datelor vizează date cu caracter personal ale unei persoane vizate care sunt inexacte. Acestui drept îi este încorporat și dreptul de a obține completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declarații suplimentare.

Răspunsul operatorului la o cerere a persoanei vizate de acest tip trebuie furnizat într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu, în special pentru orice informații adresate 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, aspectele aferente cererii formulate pot fi furnizate verbal, cu condiția ca identitatea persoanei vizate să fie dovedită prin alte mijloace. De asemenea, este necesar să se prezerve o dovadă a acțiunilor întreprinse ca urmare a cererii formulate de persoana vizată.

3. Dreptul la ștergerea datelor („dreptul de a fi uitat”)

Persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate în cazul în care se aplică unul dintre următoarele motive:

- datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate. **Spre exemplu**, persoanele, datele personale ale persoanelor vizate care nu se încadrează cerințelor postului pentru care candidează și, ca atare, prelucrarea datelor în vederea ocupării postului nu mai este necesară;
- persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea, în situația în care prelucrarea se bazează pe consimțământ sau persoana vizată își retrage consimțământul acordat explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice. De exemplu, atunci când persoana vizată și-a dat consimțământul explicit pentru crearea de statistici în vederea efectuării unor statistici a pieței muncii;
- persoana vizată se opune prelucrării în temeiul dreptului la opoziție și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea, sau persoana vizată se opune prelucrării datelor cu caracter personal care au ca scop marketingul direct. De exemplu, persoana vizată nu dorește să primească oferte de produse de la un angajator la care a susținut un interviu;
- există neclarități legate de legalitatea prelucrării datelor cu caracter personal;
- datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale care vă revine, în calitate de operator;
- datele cu caracter personal aparțin unor copii cu vârsta sub 16 ani.

GDPR a reglementat situațiile în care operatorul a făcut publice datele cu caracter personal și este obligat, potrivit prevederilor acestuia, să le șteargă. Există situații în care datele cu caracter personal au fost preluate prin diverse motoare de căutare. În acest caz, în funcție de tehnologia disponibilă și de costul implementării, trebuie să luați „măsuri rezonabile”, inclusiv măsuri tehnice, pentru a informa toți procesatorii 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..

Potrivit GDPR, „pentru a se consolida <dreptul de a fi uitat> în mediul online, dreptul de ștergere ar trebui să fie extins astfel încât un operator care a făcut publice date cu caracter personal ar trebui să aibă obligația de a informa operatorii care prelucrează respectivele date cu caracter personal să șteargă orice linkuri către datele respective sau copii sau reproduceri ale acestora”.

Destinatar înseamnă 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. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către ONG care au statut de utilitate publică, respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării.

Așadar, dreptul la ștergere nu asigură și o aplicare absolută a „dreptului de a fi uitat“. Persoanele fizice au dreptul de a dispune de datele cu caracter personal șterse, le pot încredința unui alt ONG (dreptul la portabilitatea datelor), le pot actualiza și pregăti pentru alte tipuri de prelucrări.

Există și derogări de la dreptul de a fi uitat care nu își găsește aplicare în măsura în care prelucrarea este necesară:

- pentru exercitarea dreptului la liberă exprimare și la informare;
- pentru respectarea unei obligații legale care prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului sau pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este învestit operatorul;
- din motive de interes public în domeniul sănătății publice, atunci când 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, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical. Totuși, în cazul în care datele respective sunt prelucrate de către un profesionist supus obligației de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organisme naționale competente sau de o altă persoană supusă, de asemenea, unei obligații de confidențialitate în temeiul dreptului Uniunii sau al dreptului intern ori al normelor stabilite de organisme naționale competente;

- în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice are loc cu condiția existenței unor garanții corespunzătoare, în conformitate cu prezentul regulament, pentru drepturile și libertățile persoanelor vizate. Respectivele garanții asigură faptul că au fost instituite măsuri tehnice și organizatorice necesare pentru a se asigura, în special, respectarea principiului reducerii la minimum a datelor;
- pentru constatarea, exercitarea sau apărarea unui drept în instanță.

Comunicările efectuate în temeiul dreptului de ștergere a datelor cu caracter personal exercitat de către persoana vizată sunt gratuite. În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului repetitiv, aveți posibilitatea, fie să percepeți o taxă rezonabilă ținând cont de costurile administrative pentru comunicarea transmisă, fie să refuzați a da curs cererii. În aceste cazuri, vă revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii.

În cazul în care, din diferite motive, nu puteți să furnizați un răspuns la o cerere, trebuie să explicați solicitantului că are dreptul de a se plânge autorității de supraveghere și de a deschide o cale de atac, fără întârzieri nejustificate și în termen de cel mult o lună de la primirea cererii. La solicitarea persoanei vizate, informațiile pot fi furnizate verbal, cu condiția ca identitatea persoanei vizate să fie dovedită prin alte mijloace.

Un rol deosebit de important le revine ONG-urilor, care trebuie să asigure un nivel ridicat de respectare a regulamentului. Ele trebuie să se asigure că noile concepte introduse de regulament sunt corect reflectate raportat la documentele interne care guvernează atribuțiile și responsabilitățile angajaților. De asemenea, trebuie să se asigure că orice acțiuni avute în vedere cu privire la datele angajaților sunt conforme cu cerințele impuse de regulament, lucru valabil pentru toate procesele gestionat de operator.

4. Dreptul la restricționarea prelucrării - dreptul la portabilitatea datelor

În temeiul dreptului la portabilitatea datelor, persoana vizată trebuie să primească 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. Totuși, acest drept nu ar trebui să se aplice în cazul în care prelucrarea se bazează pe un alt temei juridic decât consimțământul sau contractul.

Prin însăși natura sa, acest drept nu ar trebui exercitat împotriva operatorilor care prelucrează date cu caracter personal în cadrul exercitării funcțiilor lor publice (de exemplu, instanțele judecătorești). Acesta nu ar trebui să se aplice în special în cazul în care prelucrarea de date cu caracter personal este necesară în vederea respectării unei obligații legale căreia îi este supus operatorul sau în cazul îndeplinirii unei sarcini care servește unui interes public sau care rezultă din exercitarea unei autorități publice cu care este învestit operatorul.

De asemenea, acest drept nu ar trebui să aducă atingere dreptului persoanei vizate de a obține ștergerea datelor cu caracter personal și limitărilor dreptului respectiv și nu ar trebui, în special, să implice ștergerea acelor date cu caracter personal referitoare la persoana vizată care au fost furnizate de către aceasta în vederea executării unui contract, în măsura în care și atât timp cât datele respective sunt necesare pentru executarea contractului.

Așadar, dreptul la portabilitatea datelor se aplică atunci când prelucrarea se bazează pe consimțământ pentru unul sau mai multe scopuri specifice sau, foarte important, atunci când 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, în măsura în care acest lucru este autorizat de dreptul Uniunii 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.

O altă situație în care se aplică dreptul la portabilitatea datelor este situația în care 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.

Ultima situație de aplicare a dreptului la portabilitatea datelor este situația în care prelucrarea este efectuată prin mijloace automate.

La nivel tehnic, ar trebui să analizați și să evaluați două căi diferite și complementare de a pune date portabile la dispoziția persoanelor vizate sau a altor operatori:

- transmiterea directă a întregului set de date portabile (sau mai multe părți extrase din setul de date global);
- un instrument automat care permite obținerea datelor relevante.

5. Dreptul la opoziție

Potrivit articolului 21 din GDPR, persoana vizată are dreptul de a se opune la prelucrarea datelor personale pentru realizarea de profiluri, prelucrarea datelor prin mijloace automate, precum și prelucrarea în scopuri științifice sau istorice.

Acest drept se poate realiza în orice moment și este un drept garantat. ONG-urile ar trebui să pună la dispoziție un formular pentru exercitarea dreptului la opoziție de către persoana vizată. Imediat după exercitarea acestuia nu ar trebui să se mai prelucreze date cu caracter personal, cu excepția cazului în care operatorul demonstrează că are

motive legitime și imperioase care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanță.

În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare științifică sau istorică sau în scopuri statistice, în conformitate cu articolul 89 alineatul (1), 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 cazului în care prelucrarea este necesară pentru îndeplinirea unei sarcini din motive de interes public.

Operatorul are la dispoziție, fără întârzieri nejustificate, o perioadă de o lună, de la primirea solicitării pentru a răspunde unei cereri de opoziție. În cazul în care primiți o cerere mai complexă, care include și alte tipuri de solicitări, această perioadă de o lună poate fi prelungită până la maximum trei luni, cu condiția ca persoana vizată să fie informată cu privire la motivele acestei întârzieri în termen de o lună de la cererea inițială.

Dacă nu se poate răspunde unei astfel de cereri, operatorul trebuie să-i aducă la cunoștință persoanei vizate că se poate adresa cu o plângere autorității de supraveghere și de a deschide o cale de atac, fără întârzieri nejustificate și în termen de cel mult o lună de la primirea cererii. Informațiile comunicate în temeiul dreptului de opoziție exercitat de către persoana vizată sunt oferite gratuit.

Dreptul persoanei vizate de a se opune este adus în mod explicit în atenția persoanei vizate și este prezentat în mod clar și separat de orice alte informații încă de la prima comunicare.

6. Dreptul de a nu fi supus unor decizii automatizate, inclusiv profilarea

Persoana vizată are dreptul de a nu face obiectul unei decizii, care poate include o măsură, care evaluează aspecte personale referitoare la persoana vizată, care se bazează exclusiv pe prelucrarea automată și care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă.

Profilarea și luarea automată a deciziilor sunt utilizate într-un număr tot mai mare de sectoare, atât private, cât și private public. Crearea de profiluri ajută la luarea deciziilor și luarea deciziilor automate cu potențialul de a influența în mod semnificativ drepturile și libertățile persoanelor vizate. Profilarea și luarea deciziilor automate pot fi utile pentru persoanele și organizațiile care oferă servicii benefice cum ar fi creșterea eficienței și economisirea de resurse.

GDPR introduce prevederi care să asigure profilarea și luarea de decizii individuale automate (indiferent dacă aceasta include sau nu profilarea) și nu sunt utilizate în moduri care au un impact nejustificat asupra drepturilor persoanelor vizate; de exemplu:

- cerințe specifice de transparență și echitate;
- obligații mai mari de responsabilitate;
- temeiuri juridice specificate pentru prelucrare;
- drepturile persoanelor fizice de a se opune profiling-ului și profilării; și
- dacă sunt îndeplinite anumite condiții, necesitatea efectuării unei evaluări a impactului privind protecția datelor.

Conceptul GDPR este că orice persoană vizată ar trebui, prin urmare, să aibă dreptul de a cunoaște și de a i se comunica în special scopurile în care sunt prelucrate datele, dacă este posibil perioada pentru care se prelucrează datele cu caracter personal, destinatarii datelor cu caracter personal, logica de prelucrare automată a datelor cu caracter personal și, cel puțin în cazul în care se bazează pe crearea de profiluri, consecințele unei astfel de prelucrări.

Bineînțeles că, crearea de profiluri ar trebui permisă în cazul în care este autorizată în mod expres în dreptul Uniunii sau în dreptul intern care se aplică operatorului și în scopul asigurării securității și fiabilității unui serviciu oferit de operator sau în cazul în care este necesară pentru încheierea sau executarea unui contract între persoana vizată și un operator sau în cazul în care persoana vizată și-a dat în mod explicit consimțământul.

Așadar, crearea de profiluri este permisă atunci când:

- este necesară pentru încheierea sau executarea unui contract între persoana vizată și un operator de date;
- este autorizată prin dreptul Uniunii 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
- are la bază consimțământul explicit al persoanei vizate.

Atunci când crearea de profiluri este necesară pentru încheierea sau executarea unui contract sau se bazează pe consimțământ, 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 intervenție umană din partea operatorului, de a-și exprima punctul de vedere și de a contesta decizia.

Cum trebuie răspuns solicitărilor privind drepturile persoanelor vizate - soluții

Operatorul (inclusiv persoana împuternicită) are la dispoziție, fără întârzieri nejustificate, o perioadă de cel mult o lună de la primirea solicitării pentru a răspunde unei cereri de exercitare a drepturilor de către persoana vizată în privința datelor cu caracter personal. În cazul în care cererea este mai complexă, sau include mai multe cereri, perioada de o lună poate fi prelungită cu încă două luni dacă este necesar, cu condiția ca persoana vizată să fie informată cu privire la motivele acestei întârzieri în termen de o lună de la primirea cererii inițiale.

În cazul în care, din diferite motive, operatorul nu ia măsuri în privința cererii depuse, acesta va informa persoana vizată, fără întârziere și în termen de cel mult o luă de la primirea cererii, cu privire la motivele pentru care nu s-au luat măsuri precum și la posibilitatea persoanei de a depune o plângere în fața unei autorități de supraveghere și de a introduce o cale de atac judiciară.

Potrivit Regulamentului, comunicarea transmisă în temeiul drepturilor exercitate de către persoana vizată trebuie oferită gratuit. 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 repetitiv, se poate percepe o taxă rezonabilă ținând cont de costurile administrative pentru comunicarea transmisă sau se poate refuza a da curs cererii. În aceste cazuri, vă revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii.

Ghid GDPR pentru ONG-uri

V. Evidența activităților de prelucrare a datelor cu caracter personal

5.1. Obligația de ținere a evidenței categoriilor activităților de prelucrare

Atât operatorul cât și persoana împuternicită de operator au obligația de a păstra o evidență a activităților de prelucrare. Aceasta poate fi scrisă sau electronică și va cuprinde toate categoriilor activităților de prelucrare desfășurate în nume propriu de către operator sau de către persoana împuternicită de operator.

De asemenea, operatorul/persoana împuternicită are/au obligația de a pune evidența întocmită la dispoziția autorității de supraveghere, la cererea acesteia, de exemplu, în cazul unui control.

Potrivit dispozițiilor Regulamentului privind protecția datelor, pentru a fi **obligatoriu** să ții o evidență cu activitățile de prelucrare pe care le efectuați, este necesară îndeplinirea **oricăreia** dintre următoarele condiții:
(1) Activitatea de prelucrare este non-ocazională (activitatea de prelucrare este periodică).
(2) Activitatea de prelucrare vizează categorii speciale de date cu caracter personal.
(3) ONG are cel puțin 250 de salariați (prezumție de prelucrare a datelor pe scară largă).
(4) Activitatea de prelucrare este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate.

Caracterul necesar și obligatoriu al evidenței rezidă din prelucrările datelor cu caracter special pe care unele ONG (preponderent cele din domeniul medical) le efectuează, din caracterul recurent al prelucrărilor, precum și din riscul potențial al unor astfel de prelucrări pentru drepturile și libertățile persoanelor vizate.

Obligativitatea ținerii evidenței cu activitățile de prelucrare efectuate nu necesită îndeplinirea cumulativă a condițiilor enunțate mai sus. Cu alte cuvinte, dacă activitatea de prelucrare nu vizează categorii speciale de date, dacă suntem în prezența unui ONG al cărui număr de salariați este situat sub pragul instituit de Regulament, DAR activitatea de prelucrare se efectuează în mod periodic, sunteți obligat la întocmirea unei asemenea evidențe.

5.2. Conținutul evidenței

Regulamentul indică în mod expres informații cu privire la conținutul unei astfel de evidențe, fiind necesar ca aceasta să conțină:

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

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

c) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, după caz, documentația care dovedește existența unor garanţii adecvate;

d) o descriere generală a măsurilor tehnice și organizatorice de securitate instituite prin raportare la stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitatea și gravitatea pentru drepturile și libertățile persoanelor fizice (*spre exemplu*, pseudonimizarea și criptarea datelor cu caracter personal, capacitatea asigurării confidențialității, integrității și disponibilității datelor personale și rezistența continue ale sistemelor și serviciilor de prelucrare ș.a.m.d).

Exemplificativ, în cuprinsul evidenței activităților de prelucrare ar trebui menționate următoarele elemente:

- detalii în legătură cu persoanele vizate (ex. angajați, colaboratori, angajați ai colaboratorilor etc.);

- categorii de activități de prelucrare (ex. calcul salarii și bonusuri angajați, angajări, organigrame, colaborări între ONG-uri etc.);
- detalii cu privire la transmiterea datelor către terți și scopul pentru care sunt transmise *(ex. informațiile sunt transmise către un alt ONG în virtutea unei colaborării etc.);*
- transferuri internaționale de date (în afara SEE/către organizații internaționale) – ex. datele sunt transmise în scopul planificării călătoriilor, în scopul întocmirii unor rapoarte de grup etc.

Subliniem că păstrarea evidenței activităților de prelucrare nu reprezintă o sarcină a responsabilului cu protecția datelor, ci a operatorului/persoanei împuternicite de operator.

5.3. Forma evidenței

Evidența menționată se formulează în scris, inclusiv în format electronic.

Important! Având în vedere că acest registru de evidență ar trebui actualizat în mod constant, o bună soluție în acest sens ar fi păstrarea în formă electronică a evidenței activităților de prelucrare. De asemenea, dincolo de obligativitatea ținerii unei asemenea evidențe, suntem de părere că orice operator care efectuează activități de prelucrare trebuie să țină evidența activităților de prelucrare, aceasta fiind utilă pentru demonstrarea respectării principiilor Regulamentului raportat la categoriile de date prelucrate.

Ghid GDPR pentru ONG-uri

VI. Responsabilul privind protecția datelor cu caracter personal (DPO) în activitatea ONG-urilor

6.1. Obligația de desemnare a unui DPO (Data protection officer); când există obligația și când nu există

Esența activității DPO-ului se regăsește în obligația impusă operatorului sau persoanei împuternicite de operator de a se asigura că DPO-ul este implicat în toate aspectele legate de protecția datelor cu caracter personal, în mod corespunzător și în timp util [art. 38 alin. (1) GDPR]. Această obligație se află în strânsă legătură cu sarcina de monitorizare a DPO-ului stabilită de art. 39 alin. (2) GDPR. Implicarea DPO-ului în toate aspectele, se referă la faptul că DPO-ul va lua la cunoștință în mod nemijlocit de toate activitățile de prelucrare, fără să fie nevoie să fie informat în mod special de operator.

Potrivit art. 37 din Regulament, pentru a fi obligatorie desemnarea unui DPO este necesară întrunirea, **în mod cumulativ**, a următoarelor condiții:

(1) Operațiunile de prelucrare sunt periodice.
(2) Operațiunile de prelucrare se referă la categorii speciale de date cu caracter personal.
(3) Operațiunile de prelucrare se fac pe scară largă (prezumție: cel puțin 250 de salariați).
(4) Operațiunile de prelucrare sunt sistematice (care se efectuează metodic și organizat).
(5) Operațiunile de prelucrare reprezintă activitatea principală a persoanei împuternicite (prin natura, domeniul de aplicare și/sau scopurile operațiunilor).

În cazul în care operatorul sau persoana împuternicită de operator este un ONG de utilitate publică, poate fi desemnat un responsabil cu protecția datelor, unic pentru mai multe dintre aceste organisme, luând în considerare structura organizatorică și dimensiunea acestora.

Responsabilul cu protecția datelor este desemnat pe baza calităților profesionale și, în special, a cunoștințelor de specialitate în dreptul și practicile din domeniul protecției datelor, precum și pe baza capacității de a îndeplini sarcinile prevăzute de Regulament. Enumerarea nu este limitativă, GDPR lăsând libertate operatorului de a stabili în sarcina DPO-ului și alte sarcini sau atribuții, cu o singură condiție, respectiv ca niciuna dintre sarcinile și atribuțiile suplimentare să nu genereze un conflict de interese [art. 38 alin. (6) GDPR].

Este important de reamintit faptul că în ceea ce privește îndeplinirea sarcinilor, DPO-ul nu primește niciun fel de instrucțiuni, neputând fi demis sau sancționat pentru îndeplinirea acestora [art. 38 alin. (3) GDPR].

GDPR mai stabilește o obligație pentru DPO, respectiv aceea de a respecta secretul și confidențialitatea în îndeplinirea sarcinilor sale [art. 38 alin. (5) GDPR].

Responsabilul cu protecția datelor poate fi un membru al personalului operatorului sau al persoanei împuternicite de operator sau poate să își îndeplinească sarcinile în baza unui contract de servicii *(situație în care DPO ar fi o persoană din exteriorul companiei).*

Operatorul sau persoana împuternicită de operator **publică** datele de contact ale responsabilului cu protecția datelor **și le comunică** autorității de supraveghere. Nu este necesară publicarea datelor de identificare a DPO-ului, precum nume, prenume sau adresă de e-mail care să conțină numele acestuia.

În ceea ce privește activitatea ONG-urilor care au statut de utilitate publică, apreciem că se impune numirea unui responsabil cu protecția datelor în cadrul acestora, având în vedere că însăși legea prevede o asemenea obligație. Facem precizarea că ONG-urile care au obținut statut de utilitate publică sunt asimilate instituțiilor publice și, așa cum bine este cunoscut, este obligatorie, în toate cazurile, desemnarea unui DPO.

Cu toate că prevederile GDPR nu disting, în situația în care prelucrați atât date cu caracter personal în calitate de operator, cât și de persoană împuternicită de operator,

puteți desemna un singur responsabil cu protecția datelor care să monitorizeze activitățile de prelucrare. Aceasta întrucât responsabilitățile sale nu diferă în funcție de calitatea de persoană împuternicită de operator sau operator.

6.2. Funcția și sarcinile DPO

În calitate de operator/persoană împuternicită aveți următoarele obligații:

- ✓ de a vă asigura că responsabilul cu protecția datelor este implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal;
- ✓ de a sprijini responsabilul cu protecția datelor în îndeplinirea sarcinilor sale, asigurându-i resursele necesare pentru executarea acestor sarcini, precum și accesarea datelor cu caracter personal și a operațiunilor de prelucrare, și pentru menținerea cunoștințelor sale de specialitate;
- ✓ de a vă asigura că responsabilul cu protecția datelor nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea acestor sarcini. De reținut că, potrivit Regulamentului, acesta nu poate fi demis sau sancționat pentru îndeplinirea sarcinilor sale. Responsabilul cu protecția datelor răspunde direct în fața celui mai înalt nivel al conducerii persoanei împuternicite de operator;
- ✓ asigurarea faptului că persoanele vizate pot contacta responsabilul cu protecția datelor cu privire la toate chestiunile legate de prelucrarea datelor lor și la exercitarea drepturilor lor în temeiul Regulamentului;
- ✓ asigurarea asupra faptului că îndeplinirea sarcinilor și atribuțiilor sale NU generează un conflict de interese (*aceasta înseamnă, în primul rând, faptul că DPO nu poate deține o funcție în cadrul organizației, prin care să stabilească scopurile și mijloacele de prelucrare a datelor cu caracter personal. Datorită organigramei specifice din cadrul fiecărei organizații, acest aspect trebuie să fie analizat de la caz la caz).*

Prin Decizia nr. 74 din 19 martie 2018, Autoritatea Națională pentru Calificări a aprobat standardul ocupațional pentru Responsabil cu protecția datelor cu caracter personal

(COR 242231). Standardul ocupațional prevede ce competențe și deprinderi trebuie să aibă un responsabil cu protecția datelor, astfel:

- informarea organizației și persoanelor vizate cu privire la drepturile și obligațiile lor în baza legislației privind protecția datelor cu caracter personal;
- monitorizarea modalității prin care organizația respectă legislația privind protecția datelor cu caracter personal și standardele specifice la care organizația a aderat;
- emiterea de recomandări și oferirea asistenței de specialitate organizației cu privire la interpretarea și aplicarea prevederilor legislației privind protecția datelor cu caracter personal;
- gestionarea relației cu autoritatea de supraveghere în domeniul protecției datelor cu caracter personal;
- respectarea principiului obiectivității în domeniul protecției datelor cu caracter personal;
- asigurarea și gestionarea registrului de evidență al prelucrării datelor cu caracter personal;
- gestionarea și coordonarea resurselor umane, financiare, tehnice necesare realizării sarcinilor și activităților specifice domeniului protecției datelor cu caracter personal;
- dezvoltarea profesională continuă în domeniul protecției datelor cu caracter personal;
- monitorizarea aplicării instrumentelor și metodelor de îmbunătățire a eficacității sistemului de management al securității informației;
- analizarea și evaluarea riscurilor de prelucrare a datelor cu caracter personal.

În ceea ce privește ocuparea funcției de DPO în cadrul unui ONG, precizăm, ca regulă generală, că printre funcțiile care pot genera un conflict de interese din cadrul organizației se pot include funcțiile personalului de conducere de nivel superior (*precum funcția de președinte al unei asociații sau fundații,* precum și alte funcții de rang inferior în cadrul unui ONG dacă astfel de poziții sau roluri conduc la stabilirea scopurilor și mijloacelor de prelucrare. În plus, ar putea să apară un conflict de interese, spre exemplu, dacă i se solicită unui DPO de la nivel extern să vă reprezinte în cauze care implică probleme legate de protecția datelor.

Recomandăm ca problematica conflictului de interese să fie analizată **de la caz la caz**, în funcție de organizarea și funcționarea ONG-ului, ținând cont și de volumul activităților de prelucrare.

Responsabilul cu protecția datelor are cel puțin următoarele **sarcini:**

- ✓ informează și consiliază operatorul de date cu caracter personal, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul Regulamentului;
- ✓ monitorizează respectarea Regulamentului și a politicilor operatorului în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;
- ✓ furnizează consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia;
- ✓ cooperează cu autoritatea de supraveghere;
- ✓ asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă prevăzută de Regulament, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune;
- ✓ va putea fi contactat de către persoanele vizate în ceea ce privește chestiunile legate de prelucrarea datelor lor și exercitarea drepturilor aferente Regulamentului;
- ✓ obligația de respectare a secretului sau confidențialității în ceea ce privește îndeplinirea sarcinilor sale.

Funcția de DPO este o funcție complexă ce necesită atenție și preocupare constantă. Pentru îndeplinirea corectă a sarcinilor sale, responsabilul cu protecția datelor ar trebui să manifeste maximă diligență și să țină seama întotdeauna de natura și specificul activităților de prelucrare efectuate de operator.

VII. Evaluarea impactului asupra protecției datelor (DPIA)

7.1. Evaluarea impactului asupra protecției datelor

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.

Pentru a se efectua DPIA, DPO-ul ar trebui să acorde asistență operatorului în ceea ce privește impactul asupra protecției datelor, și anume:
– ce metodologie să urmeze operatorul la realizarea unei DPIA;
– dacă să se realizeze DPIA intern sau să se externalizeze;
– ce garanții (inclusiv măsurile tehnice și organizatorice) să le aplice pentru a atenua orice riscuri pentru drepturile și interesele persoanelor vizate;
– dacă evaluarea impactului privind protecția datelor a fost sau nu efectuată corect;
– dacă este vorba de concluziile sale (dacă trebuie sau nu să se desfășoare sau nu prelucrarea și ce măsuri de protecție pentru a aplica) sunt în conformitate cu GDPR.

Regulamentul prevede o listă exemplificativă a situațiilor în care prelucrarea datelor personale prezintă un risc ridicat asupra drepturilor și libertăților fundamentale ale persoanelor vizate și, prin urmare, trebuie trecută prin filtrul unei evaluări DPIA, și anume:

- ✓ în cazul unei **prelucrări sistematice și cuprinzătoare a aspectelor personale** referitoare la persoane fizice (*spre exemplu, situația economică*), care se bazează pe **prelucrarea automată**, inclusiv crearea de profiluri, și care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;
- ✓ în cazul **prelucrării pe scară largă a unor categorii speciale de date**; sau
- ✓ în cazul unei **monitorizări sistematice pe scară largă** a unei zone accesibile publicului.

Cu titlu exemplificativ, menționăm criteriile care pot fi avute în vedere în scopul determinării dacă prelucrarea se face sau nu la „*scară largă*”, și anume:

- ✓ numărul persoanelor vizate;
- ✓ volumul datelor cu caracter personal prelucrate;
- ✓ durata prelucrării datelor cu caracter personal;
- ✓ aria geografică a activității de prelucrare.

Procedura de evaluare a impactului asupra protecției datelor constă cel puțin în următoarele aspecte:

- ✓ descrierea procesului de prelucrare a datelor, respectiv a operațiunilor de prelucrare, inclusiv a scopului acesteia și a interesului legitim urmărit de operator;
- ✓ evaluarea necesității și proporționalității operațiunilor de prelucrare în legătură cu scopurile avute în vedere;
- ✓ identificarea posibilelor amenințări asupra drepturilor persoanelor fizice și evaluarea riscurilor;
- ✓ evaluarea soluțiilor pentru îndepărtarea riscurilor, respectiv a măsurilor de securitate – trebuie adoptate decizii cu privire la fiecare identificat.

Autoritatea națională de supraveghere va veni în sprijinul dumneavoastră prin publicarea unor liste care să conțină tipurile de prelucrări care trebuie să fie supuse unei evaluări DPIA, dar și tipurile de prelucrări care nu trebuie evaluate.

Procedura DPIA se realizează de către operator și trebuie coordonată de persoane care cunosc foarte bine proiectele pe care le aveți în derulare, însă poate fi și externalizată în cazul în care doriți să vă consultați cu un specialist în domeniu.

Anexa 2 a Ghidului DPIA a Grupului de Lucru Art. 29 sprijină operatorii și persoanele împuternicite prin indicarea punctelor pe care trebuie să le atingă procedura, în concordanță cu exigențele Regulamentului general privind protecția datelor.

7.2. Consultarea prealabilă

În cazul în care evaluarea indică faptul că prelucrarea datelor cu caracter personal ar genera un risc ridicat asupra drepturilor și libertăților persoanelor fizice vizate, iar operatorul consideră că riscul nu poate fi atenuat prin mijloace rezonabile de securitate, acesta trebuie să se adreseze autorității de supraveghere pentru consultare.

În acest scop, veți depune la autoritate concluziile raportului de evaluare împreună cu măsurile propuse pentru atenuarea riscurilor, dar și alte informații prevăzute în art. 36 alin. (3) din Regulament, și anume:

- ✓ responsabilitățile respective ale operatorului și ale persoanelor împuternicite de operator implicate în activitățile de prelucrare;
- ✓ scopurile și mijloacele prelucrării preconizate;
- ✓ măsurile și garanțiile prevăzute pentru protecția drepturilor și libertăților persoanelor vizate;
- ✓ dacă este cazul, datele de contact ale responsabilului cu protecția datelor;
- ✓ evaluarea impactului asupra protecției datelor; și
- ✓ orice alte informații solicitate de autoritatea de supraveghere.

Atunci când consideră că prelucrarea în aceste condiții ar încălca Regulamentul, în special atunci când riscul nu a fost identificat sau atenuat într-o măsură suficientă de către operator, autoritatea de supraveghere **oferă consiliere în scris** operatorului și, după caz, persoanei împuternicite de operator, în cel mult opt săptămâni de la primirea cererii de consultare, și își poate utiliza oricare dintre competențele menționate la articolul 58 *(de a efectua activități de investigare, corective, autorizare și consiliere).* Această perioadă poate fi prelungită cu șase săptămâni, ținându-se seama de complexitatea prelucrării prevăzute.

Autoritatea de supraveghere informează operatorul și, după caz, persoana împuternicită de operator, în termen de o lună de la primirea cererii, cu privire la orice astfel de prelungire, prezentând motivele întârzierii. Aceste perioade pot fi suspendate până când

autoritatea de supraveghere a obținut informațiile pe care le-a solicitat în scopul consultării.

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

În opinia noastră, evaluarea impactului asupra protecției datelor cu caracter personal reprezintă o procedură-cheie ori de câte ori considerați că ar putea exista un risc cu privire la operațiunile de prelucrare a unor date sensibile, prelucrare care ar putea produce prejudicii asupra drepturilor persoanelor fizice vizate, dar și asupra dumneavoastră, în calitate de operator/persoană împuternicită. Punerea în aplicare a unei metodologii corecte de evaluare vă va ajuta în respectarea conformității cu rigorile impuse de Regulament, dar și cu actele normative/regulile care vor fi emise de autoritățile de supraveghere în scopul implementării acestuia.

CONCLUZII

Lăsând la o parte aplicarea GDPR în mediul economic, de business și în cadrul instituțiilor statului, apreciem că se impune ca accentul să fie pus pe implicațiile în mediul ONG unde există un **volum imens de date cu caracter personal** care, în majoritatea cazurilor, este gestionat în moduri necorespunzătoare și expus riscurilor.

Întreaga lume se bazează pe organizații non-profit pentru a furniza servicii sensibile comunitare, inclusiv asistența medicală primară, educație, locuințe, refugiați și imigranți etc. Organizațiile non-profit au aderat din ce în ce mai mult la tehnologie pentru a îmbunătăți eficiența acestora și de a extinde aria de incidență și accesibilitatea la acestea. Multe organizații non-profit nu au început să își concentreze atenția asupra securității și planificării protecției datelor cu caracter personal. Această lipsă de atenție ar putea expune organizația non-profit unor riscuri de securitate și de reglementare pe care majoritatea entităților pur și simplu nu și le pot permite.

GDPR vine cu noi reglementări privind stocarea, prelucrarea și tranzitul de date cu caracter personal în cadrul și între statele membre UE. Vom aminti doar câteva aspecte esențiale cu aplicabilitate în mediul ONG și posibilele sancțiuni în cazul nerespectării normelor:

- Persoana vizată, fie că este voluntar, angajat, colaborator, beneficiar, donator, trebuie să își dea acordul explicit asupra modului în care ii vor fi prelucrate datele personale *(această chestiune este atenuată de dispozițiile art. 9 din Legea nr. 190/2018 în care se prevede că organizațiile non-profit nu trebuie să obțină consimțământul persoanelor vizate pentru prelucrările efectuate în îndeplinirea obiectivelor sale, date care să se refere la membrii organizației sau la persoanele care au legătură cu organizația).*
- Persoana vizată trebuie să fie informată cu privire la drepturile pe care le are, privind actualizarea, modificarea, ștergerea datelor cu caracter personal, precum și cu privire la dreptul de a consulta datele personale ori de câte ori are nevoie.

- Persoana vizată trebuie informată în mod explicit cu privire la căile de a se opune prelucrării, cât și cu privire la căile legale de atac.
- Persoana vizată are dreptul de a fi „uitată”, adică de a-i fi eliminate sau anonimizate datele personale, astfel ca identificarea persoanei să devină imposibilă.
- Operatorul de date cu caracter personal trebuie să asigure condiții de păstrare în siguranță a datelor, după noi standarde care pot implica după caz upgrade-ul sistemului informatic și/sau de gestiune a datelor cu caracter personal, de unde deducem că vor exista costuri de implementare la nivel de entitate juridică.
- Entitatea va trebui să raporteze orice incident legat de sistemele de gestiune a datelor cu caracter personal. Ex: atac informatic, pătrundere prin efracție, scurgeri de date constatate etc.
- Entitatea va trebui să-și organizeze datele de așa natură încât să asigure portabilitatea acestora. Mai exact, persoana vizată poate solicita exportul datelor într-un format agreat general, în scopul importului/transferului în alt sistem. Ex: fișier Excel, fișier CSV, bază de date etc.
- În anumite cazuri se poate impune angajarea sau instruirea unei persoane care să îndeplinească funcția și rolul de Responsabil cu protecția datelor cu caracter personal, cu întregile responsabilități ce îi revin conform legii.
- În domeniul online, utilizatorii/vizitatorii website-ului organizației trebuie să-și dea acordul în mod explicit privind prelucrarea datelor cu caracter personal, chiar dacă este vorba doar de adresa de e-mail folosită la crearea unui cont de utilizator sau completarea unui formular de contact.
- De asemenea, nu vor fi acceptate câmpurile precompletate, precum „bifa” de abonare la newsletter/știri. Astfel de bife vor fi puse de utilizator, excluzând astfel riscul trecerii din neatenție peste un câmp prebifat. Valabil și pentru acceptarea termenilor de utilizare, a termenilor legali, a politicii de cookie-uri, a politicii de confidențialitate etc.
- Tot în domeniul online, proprietarul website-ului trebuie să demonstreze că dispune de măsuri de securitate privind stocarea și prelucrarea datelor cu caracter personal, aspectul răsfrângându-se și asupra entității care găzduiește website-ul. Astfel că proprietarul website-ului ar trebui să-și contacteze găzduitorul și să

obțină o declarație privind modul în care îi sunt securizate datele cu caracter personal stocate în cadrul website-ului și/sau al bazei/bazelor de date aferente.

Supunem atenției faptul că implicațiile aplicării GDPR vor fi majore, iar nerespectarea normelor se va taxa cu amenzi uriașe. Nu vrem să vehiculăm sumele de milioane de euro specificate pentru mediul economic, dar nici ONG-urile nu vor fi scutite de amenzi uriașe.

Știm că în domeniul ONG legislația este mai relaxată, inclusiv ca aplicare, știm că multe ONG-uri aplică cu mai puțină rigurozitate legislația în materie, astfel că luarea în considerare a unui semnal de alarmă în timp util se va dovedi a fi benefic.

ONG-urile vor trebui să fie foarte atente atunci când stochează și prelucrează date cu caracter personal, vor trebui să aibă acordul explicit al persoanelor vizate, de preferat în scris sub semnătura, indiferent că este vorba de voluntari, angajați, colaboratori sau beneficiari ai campaniilor umanitar-caritabile.

Și ca să ne exprimăm plastic, o ultimă precizare asupra posibilelor riscuri: noua norma va exacerba spiritul procesoman. Astfel de acțiuni deja au loc, cu consecințe grave asupra entităților reclamate. Vă sfătuim să vă asigurați din timp cadrul legal, să vă consultați avocați și juriști, astfel ca să minimizați efectele posibilelor nerespectări ale normelor și ale potențialelor reclamații.

DE REȚINUT:	
Ale cui și ce date cu caracter personal prelucrați?	*Exemple:* Datele membrilor, datele persoanelor înscrise la newsletter, datele vizitatorilor paginii web, datele vizitatorilor paginii de Facebook, datele angajaților, datele suporterilor sau susținătorilor, datele participanților la un eveniment etc. *Exemple:* date facturare, date de contact, date de identificare, date privind sănătatea etc.
Legalitate – pe ce bază prelucrați datele personale?	Consimțământul persoanelor vizate. Câteodată, însă, acordul este greu de luat (uneori persoana se poate și răzgândi, deci nu vă puteți baza pe consimțământ). Pe lângă consimțământ, se poate apela la: încheierea unui contract între două părți, obligația legală care îi revine operatorului, interesul legitim al operatorului. ***Exemple:*** datele cu caracter personal necesare transmiterii unui newsletter se bazează pe consimțământ, datele personale inserate într-un contract folosesc la încheierea acordului dintre cele două părți, datele cu caracter personal utilizate pentru completarea unei facturi poate reprezenta o obligație legală; datele cu caracter personal (inclusiv imagini) obținute

	de la un eveniment se colectează, de obicei, pe bază de consimțământ.
Cui divulgați datele cu caracter personal colectate? *(cine altcineva mai are acces la date, pe lângă ONG)*	Există două entități diferite care pot avea acces la date: operatorul *(persoana fizică sau juridică care, singură sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal. De obicei, operatorul este ONG-ul)* sau persoana împuternicită de operator *(persoana fizică sau juridică care prelucrează datele în numele operatorului, adică un intermediar ca: programatorii care lucrează la un website, un software, un furnizor de marketing, furnizor de servicii contabile, un finanțator sau orice alt terț)*. În momentul în care ONG-ul apelează la o persoană împuternicită, trebuie să existe un contract scris (pe hârtie sau electronic) care să precizeze în ce situații acea persoană poate să prelucreze datele respective. Desigur, persoanele împuternicite de operator nu au dreptul să divulge datele colectate către alte persoane, cu excepția aplicabilității unor norme legale care obligă în acest sens.
	Nu există o listă finală și fixă de măsuri pentru securitatea prelucrării datelor, deci este la latitudinea operatorului, în funcție de datele colectate și în funcție de

Ce măsuri luați pentru a asigura securitatea datelor?	capacitatea de a face față anumitor măsuri (ex.: pe care să și le permită). O măsură organizatorică pentru a spori securitatea ar putea fi ca doar anumite persoane din organizație (în special în organizațiile mari) să aibă acces la datele cu caracter personal. Din categoria de măsuri tehnice care se pot lua pentru protecția datelor cu caracter personal face parte, de exemplu, parolarea bazei de date, criptarea, pseudonimizarea etc. Angajații ONG-urilor care prelucrează date cu caracter personal ar trebui să aibă clauze de confidențialitate în contracte. Clauze similare se pot stabili și în cazul terților care au acces la datele cu caracter personal.
Puteți să informați ANSPDCP în cazul încălcării securității datelor?	Regulamentul UE a introdus obligația ca, dacă există o încălcare a securității datelor *(nu neapărat o pierdere a lor, ci inclusiv faptul că cineva neautorizat a avut acces la acele date),* în termen de 72 de ore de la încălcare Autoritatea să fie notificată. Este posibil ca momentul în care este sesizată această încălcare de către operator să fie foarte îndepărtat. Chiar și așa, trebuie să fie notificată Autoritatea (există posibilitatea chiar ca Autoritatea să oblige la notificarea persoanelor ale căror date au fost pierdute sau compromise).

ANEXA 1: SECURITATEA DATELOR CU CARACTER PERSONAL. MĂSURI TEHNICE ȘI ORGANIZATORICE

Un principiu-cheie al RGPD este acela conform căruia prelucrarea datelor cu caracter personal trebuie să fie efectuată în condiții de siguranță, și anume, prin instituirea unor „măsuri tehnice și organizatorice corespunzătoare” - principiul securității datelor cu caracter personal.

Încălcarea securității datelor cu caracter personal înseamnă o încălcare a securității care duce la distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal, în mod accidental sau ilegal.

Aceasta include încălcările cauzate atât în mod accidental, cât și în mod intenționat. De asemenea, acest lucru înseamnă că o încălcare este mai mult decât o simplă pierdere a datelor cu caracter personal.

Încălcările securității datelor cu caracter personal pot cuprinde:

- accesul unui terț neautorizat;
- acțiunea (sau inacțiunea) intenționată sau accidentală a unui operator sau a unei persoane împuternicite de operator;
- trimiterea unor date cu caracter personal către un destinatar greșit;
- pierderea sau furtul unor dispozitive informatice care conțin date cu caracter personal;
- modificarea datelor cu caracter personal fără permisiune;
- pierderea disponibilității datelor cu caracter personal.

RGPD vă solicită să luați în considerare să efectuați analize de risc și să implementați politici organizatorice și măsuri fizice și tehnice. De asemenea, trebuie să luați în considerare cerințe suplimentare în privința securității prelucrărilor pe care le efectuați.

În momentul în care vă decideți ce măsuri de securitate implementați – este recomandat să aveți în vedere modalitatea și costurile punerii lor în aplicare, astfel încât acestea să fie corespunzătoare atât specificului activității dumneavoastră, cât și riscurilor pe care le prezintă prelucrările.

Acolo unde este cazul, ar trebui să luați măsuri de securizare a datelor cu caracter personal, cum ar fi pseudonimizarea și criptarea lor.

Măsurile pe care doriți să le implementați trebuie să asigure „confidențialitatea, integritatea și disponibilitatea" sistemelor și serviciilor și a datelor cu caracter personal pe care le prelucrați prin acestea.

De asemenea, măsurile pe care decideți să le implementați trebuie să fie de natură a permite restabilirea accesului și disponibilității datelor cu caracter personal în timp util în eventualitatea producerii unui incident fizic sau tehnic.

Trebuie să vă asigurați că aveți implementate procese corespunzătoare prin care să puteți testa eficiența măsurilor implementate și care să vă ajute la efectuarea oricăror îmbunătățiri necesare.

În acest sens:

- Trebuie să întreprindeți o analiză a riscurilor prezentate de prelucrările pe care le efectuați, și le veți folosi pentru a evalua nivelul adecvat de securitate de care aveți nevoie pentru a-l pune în aplicare.
- Trebuie să aveți o politică de securitate sau un document echivalent acesteia și să vă asigurați că această politică este implementată.
- Când vă decideți în privința măsurilor pe care trebuie să le implementați, trebuie să luați în considerare modalitatea și costurile implementării.
- Când este cazul, este recomandat să aveți politici suplimentare care să asigure că mecanismele de control sunt pregătite a fi puse în aplicare.
- Trebuie să vă asigurați că, în mod regulat, revizuiți informațiile și măsurile politicilor de securitate și, atunci când este cazul, să le îmbunătățiți.

 Trebuie să aveți instituite comenzi tehnice de bază.

 Trebuie să aveți în vedere în permanență faptul că s-ar putea să aveți nevoie și de alte măsuri tehnice depinzând de circumstanțele activității dumneavoastră și de tipul datelor cu caracter personal pe care îl prelucrați.

 Ca recomandare, ar fi bine să utilizați criptarea sau pseudonimizarea datelor.

 Sunteți conștient de cerințele RGPD în privința confidențialității, integrității și disponibilității datelor cu caracter personal pe care le prelucrați.

 Trebuie să organizați teste regulate și revizii asupra măsurilor implementate pentru a vă asigura că acestea se mențin în continuare eficiente, și să întreprindeți îmbunătățiri asupra acelor teste care semnalează zone asupra cărora se pot aduce îmbunătățiri.

 Acolo unde este cazul, este recomandabil să implementați măsuri care aderă la un cod de conduită aprobat sau mecanism de certificare.

 Trebuie să vă asigurați că operatorii implementează la rândul lor măsuri tehnice și organizatorice corespunzătoare.

RGPD impune ca prelucrările datelor cu caracter personal să aibă loc într-un cadru securizat, precizând într-un mod specific ce trebuie să faceți în această privință și cum ar trebui să evaluați eventualele riscuri, precum și, în mod corelativ, cum să instituiți măsurile securitate adecvate. Deși până în prezent, aceste chestiuni nu au fost întru totul străine, în baza unor bune practici care stăteau la baza instituirii lor, acum ele reprezintă o cerință legală.

Articolul 5 alin. (1) lit. f) din RGPD vorbește despre ***„integritatea şi confidențialitatea”*** datelor cu caracter personal, în sensul că acestea ar trebui: „procesate într-o manieră care să asigure securitatea corespunzătoare a datelor cu caracter personal, incluzând protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii accidentale, distrugerii sau deteriorării, folosind măsuri tehnice sau organizatorice adecvate” – principiul RGPD, în sens larg, în privința securității datelor cu caracter personal.

Acest lucru înseamnă că trebuie să aveți o securitate corespunzătoare pentru a preveni compromiterea datelor cu caracter personal pe care le dețineți, în mod accidental sau intenționat. Trebuie să aveți în vedere faptul că, de vreme ce securitatea informațiilor

este considerată ca fiind noțiunea de „cybersecurity” (protecția rețelelor și a sistemelor informatice împotriva unui atac), aceasta include, de asemenea, și alte lucruri, cum ar fi măsuri fizice și organizatorice.

Astfel, principiul securității datelor cu caracter personal trebuie interpretat în corelație cu articolul 32 din RGPD, care detaliază securitatea prelucrărilor datelor cu caracter personal. Articolul 32 alin. (1) statuează: „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”.

Principiul securității datelor este incident dincolo de modul în care stocați sau transmiteți date cu caracter personal. Orice aspect al prelucrărilor datelor cu caracter personal trebuie să fie acoperit, nu doar rețelele și sistemele informatice „cybersecurity”. Acest lucru înseamnă că măsurile de securitate pe care le instituiți ar trebui să asigure faptul că:

- datele cu caracter personal pot fi accesate, alterate, dezvăluite sau șterse doar de către cei care sunt autorizați să facă asta (și că acești oameni acționează în conformitate cu instrucțiunile pe care le dați);
- datele cu caracter personal pe care le dețineți sunt corecte/actualizate și complete în relație cu scopul pentru care le prelucrați; și
- datele cu caracter personal rămân accesibile și utilizabile, dacă acestea, în mod accidental sunt pierdute, alterate sau distruse, astfel că trebuie să fiți capabil să le recuperați și mai mult decât atât, să preveniți orice efect negativ, primejdie asupra persoanelor vizate implicate.

Aceste aspecte sunt cunoscute sub noțiunile de **„confidențialitate, integritate și disponibilitate”** și, sub imperiul RGPD, fac parte din obligațiile dumneavoastră.

RGPD nu definește măsurile de securitate pe care ar trebui să le implementați, ci solicită să aveți un nivel al securității care să fie „adecvat” riscurilor pe care le prezintă prelucrările.

Trebuie să aveți în vedere, în acest sens, modalitatea concretă și costurile implementării, precum și natura, scopul, contextul prelucrărilor.

Acest aspect reflectă conceptul RGPD al abordării bazate pe risc, în sensul că nu există nicio soluție unică care să se potrivească tuturor prelucrărilor pentru securitatea datelor cu caracter personal. Înseamnă că ceea ce poate fi „corespunzător” pentru compania dumneavoastră va depinde de specificul activității, de prelucrările pe care le efectuați și riscurile pe care le prezintă acestea companiei dumneavoastră.

Așadar, înainte de a decide care măsuri sunt corespunzătoare spre a fi implementate, trebuie să evaluați mai întâi riscurile. Ar trebui să revizuiți datele cu caracter personal pe care le dețineți și modul în care le utilizați pentru a evalua cât de valoroase sunt acestea, dacă sunt date sensibile sau confidențiale - la fel ca și daunele sau dezvăluirile care pot fi produse dacă acestea ar fi compromise. De asemenea, ar trebui să țineți cont de următorii factori:

- natura și extinderea sediilor organizației dumneavoastră și a sistemelor informatice;
- numărul personalului pe care îl aveți și amploarea accesului pe care îl au la datele personale; și
- orice date cu caracter personal deținute sau folosite de către persoana împuternicită care acționează în numele dumneavoastră.

Efectuarea unei evaluări a riscurilor este un exemplu de măsură organizatorică, dar veți avea nevoie să luați, de asemenea, și alte măsuri. Ar trebui să aveți ca obiectiv principal construirea unei culturi de conștientizare a securității la nivelul companiei dumneavoastră. În acest sens, ar trebui să identificați o persoană care să aibă responsabilitatea zilnică pentru securitatea datelor în cadrul companiei și să vă asigurați

că această persoană are la dispoziție resursele și autoritatea corespunzătoare pentru a-și îndeplini sarcinile în mod efectiv.

Responsabilitatea stabilită în mod clar în privința securității vă va asigura că nu au fost trecute cu vederea anumite probleme, și că starea generală de securitate nu a devenit defectuoasă sau depășită de realitate.

În continuare, va trebui să aveți în vedere și alte chestiuni conexe, cum ar fi:

 coordonarea între personalul-cheie din cadrul companiei (managerul de securitate va trebui să știe despre punerea în funcțiune și va trebui să dispună de orice echipamente IT);
 accesul în sediile companiei sau echipamentele acesteia acordat unei persoane din afara companiei (spre exemplu, pentru servicii de mentenanță) și considerentele suplimentare de securitate pe care acest lucru le va genera;
 continuitatea aranjamentelor de business care să identifice cum trebuie să vă protejați și/sau să recuperați orice date personale pe care le dețineți;
 verificări periodice pentru a vă asigura că măsurile de securitate rămân actuale și la același nivel corespunzător.

Măsurile tehnice sunt uneori considerate ca reprezentând protecția datelor personale deținute în dispozitive și rețele. În timp ce acestea sunt de o importanță evidentă, multe incidente de securitate se pot produce din cauza furtului sau pierderea echipamentului, abandonul dispozitivelor vechi sau pierderea, furtul copiilor înregistrate sau eliminarea incorectă a lor. Prin urmare măsurile tehnice includ atât măsuri de securitate fizică, cât și cele de IT.

Atunci când aveți în vedere măsurile de securitate fizică, ar trebui să luați în considerare factori precum:

 calitatea ușilor și a încuietorilor și protecția sediilor companiei prin alarme, iluminat de siguranță sau CCTV;

- cum controlați accesul în sediile companiei, și în ce modalitate sunt supravegheați vizitatorii;
- cum păstrați echipamentul IT, dispozitivele mobile particulare.

În ceea ce privește sistemele IT, măsurile tehnice sunt cele privitoare la „cybersecurity” – o arie tehnică complexă care evoluează în mod constant, cu noi amenințări și vulnerabilități întotdeauna în curs de dezvoltare. Prin urmare, este rezonabil să presupunem că sistemele companiei dumneavoastră informatice sunt vulnerabile și este nevoie să luați măsuri pentru a le proteja.

Atunci când aveți în vedere „cybersecuritatea”, ar trebui să luați în considerare factoriprecum:

- sistemul de securitate – securitatea rețelei și a informațiilor din sistem, inclusiv pe acelea care prelucrează date cu caracter personal, instalarea și updatarea constantă a antivirusului folosit;
- securitatea datelor – securitatea datelor pe care le deținești prin sistemele dumneavoastră, asigurând un control de acces și deținerea în siguranță a datelor;
- securitatea online – securitatea website-urilor și oricărui alt serviciu/aplicație online pe care o folosiți și
- securitatea device-urilor – incluzând politici cu privire la „bring-your-own-device” (BYOD) dacă îl oferiți.

Măsurile de securitate în privința protecției datelor cu caracter personal pe care le implementați ar trebui să aibă ca rezultat garantarea confidențialității, integrității, disponibilității pentru fiecare sistem și pentru fiecare prelucrare de date.

De asemenea, trebuie să aveți abilitatea să asigurați „capacitatea de adaptare” a sistemelor informatice care efectuează prelucrări de date.

Capacitatea de adaptare se referă la:

 proprietatea sistemelor informatice ale companiei să continue să funcționeze în condiţii nefavorabile, cum ar fi cele care pot rezulta în urma unui incident fizic sau tehnic; și
 proprietatea sistemelor de a se restaura la o stare efectivă de funcționare.

Trebuie să aveți abilitatea de restaurare a disponibilității datelor și a accesului la acestea în situația unui incident fizic sau tehnic în mod corespunzător și într-un timp scurt (ex: inundație, incendiu, pană de curent).

Personalul companiei

Trebuie să vă asigurați că oricine acționează cu drept de acces la datele cu caracter personal nu prelucrează date personale decât în situația în care l-ați instruit cum să procedeze în acest sens. Prin urmare, este vital ca personalul angajat din cadrul companiei dumneavoastră să înțeleagă importanța protejării datelor cu caracter personal, să fie familiarizat cu Politica de securitate și procedurile ce trebuie puse în practică.

Ar trebui să oferiți formare inițială și perfecționare continuă adecvată, incluzând:

 responsabilitățile dumneavoastră ca operator/persoană împuternicită de operator sub imperiul RGPD;
 responsabilitățile personalului pentru protecția datelor – incluzând explicarea consecințelor prelucrării deficitare a datelor personale, inclusiv de comitere a unor fapte penale, în cazul în care încearcă în mod deliberat să acceseze sau să divulge aceste date fără drept;
 pericolele ce decurg din încercările diverselor persoane de a obține date personale prin înșelăciune (de exemplu, pretinzând că ar fi persoanele la care datele se referă, sau permisiunea personalului să recunoască atacurile de „tip phishing, social engineering, malware”); și
 orice restricții plasate pe dispozitivele personale utilizate de personalul companiei (de exemplu, pentru a evita infectarea cu virus sau spam).

Instruirea personalului va fi eficace doar în cazul în care persoanele cărora se adresează furnizează, la rândul lor, încredere, adaptabilitate și cunoștințe, și dacă formarea acestora este continuă.

Notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal

Stabilirea unei astfel de obligații în sarcina dumneavoastră, în calitate de operator, este relevantă pentru a vă responsabiliza, pe de o parte, făcându-vă conștient de faptul că măsurile de securitate adoptate anterior producerii incidentului nu au fost suficiente, fiind necesară o reevaluare a acestora, iar pe de altă parte, pentru a vă sprijini, cu ajutorul autorității de supraveghere, în a identifica, în circumstanțele incidentului, toate riscurile produse și a le gestiona în mod corect, spre a reduce posibilele prejudicii actuale sau viitoare. Prin urmare, singura excepție admisă pentru a nu fi notificat un incident de securitate se referă la situația în care încălcarea nu prezintă riscuri pentru drepturile salariatului.

GDPR prevede nu numai cine sunt titularii obligației de notificare (operatorii de date cu caracter personal), dar și termenul în care trebuie îndeplinită această obligație, precum și conținutul unei astfel de notificări.

Operatorul rămâne responsabil și este ținut de această obligație chiar și atunci când prelucrează date cu caracter personal prin intermediul unei persoane împuternicite la nivelul căreia s-ar fi produs incidentul în cauză. Într-un atare caz, este important ca în cadrul instrucțiunilor ce sunt date persoanei împuternicite (încă de la data desemnării sale printr-un contract sau alt act juridic) să fie trasată foarte clar și distinct obligația acesteia de a-l anunța pe operator de îndată ce a avut loc un incident (de orice tip), pentru a-i putea da acestuia din urmă posibilitatea de a-l analiza în timp util și de a transmite notificarea în termenele strict prevăzute de Regulament.

Termenul prevăzut de Regulament pentru efectuarea notificării este generic „fără întârzieri nejustificate”; însă se stabilește, totodată, limita maximă a unui termen de cel mult 72 de ore („dacă este posibil”) de la data la care operatorul a luat cunoștință de producerea incidentului (ca urmare a unei notificări din partea persoanei împuternicite, a unei sesizări provenite de la persoanele afectate ori din mass-media, pe baza propriilor constatări etc.).

În cazul în care termenul maximal prevăzut este depășit, este necesar să fie indicate motivele pentru care notificarea se realizează cu depășirea celor 72 de ore.

Notificarea făcută la autoritatea de supraveghere are un conținut minimal, prevăzut de Regulament:

- ✓ descrierea caracterului încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil:
- ✓ categoriile și numărul aproximativ al persoanelor vizate în cauză;
- ✓ categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;
- ✓ numele și datele de contact ale responsabilului cu protecția datelor (dacă organizația dumneavoastră are un asemenea responsabil) sau un alt punct de contact de unde se pot obține mai multe informații;
- ✓ descrierea consecințelor probabile ale încălcării securității datelor cu caracter personal;
- ✓ descrierea măsurilor luate sau propuse spre a fi luate pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile luate pentru atenuarea eventualelor efecte negative.

În situația în care nu este posibil ca de la început să poată fi comunicate toate aceste informații, este admisă și notificarea în etape, fără întârzieri nejustificate.
Pentru toate incidentele produse (inclusiv pentru cele care nu au atras transmiterea notificării), operatorul este obligat să mențină o documentație adecvată (situația de fapt, consecințe produse și măsuri de remediere), care să poată fi pusă la dispoziția autorității

de supraveghere în cazul efectuării unui control, pentru a verifica conformitatea la obligațiile impuse de Regulament.

Ce se întâmplă dacă nu transmiteți notificarea?

- netransmiterea notificării cu privire la o încălcare, atunci când aceasta este obligatorie, poate conduce la o amendă considerabilă, de până la 10 milioane Euro sau 2% din cifra dumneavoastră de afaceri globală.
- amenda poate fi combinată cu celelalte competențe corective ale ANSPDCP conform art. 58.
- așadar, este important să vă asigurați că ați implementat un proces solid de raportare a încălcărilor pentru a fi siguri că depistați și că puteți notifica o încălcare la timp, precum și pentru a furniza datele necesare.

Informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal

Spre deosebire de notificarea care trebuie transmisă autorității de supraveghere, în acest caz, operatorul este ținut să notifice persoanele lezate numai în situația producerii unui risc ridicat pentru drepturile și libertățile acestora.

În vederea unei evaluări obiective a gradului de risc, GDPR apreciază în funcție de existența unor prejudicii fizice, materiale sau morale (spre exemplu, discriminare, furt de identitate, fraudă, pierderi financiare, atingeri aduse reputației), iar drept criterii pentru a diferenția un risc obișnuit de unul ridicat pot fi luate în considerare elemente precum:

- ✓ tipul încălcării;
- ✓ natura și volumul datelor afectate;
- ✓ posibilitatea de identificare a persoanelor;
- ✓ severitatea consecințelor;
- ✓ caracteristici specifice persoanelor;
- ✓ numărul persoanelor afectate;
- ✓ caracteristici ale operatorului.

În ceea ce privește termenul în care notificarea trebuie realizată, acesta este unul mult mai strict, respectiv „fără întârzieri nejustificate”, tocmai pentru a da posibilitatea persoanelor afectate de a aprecia la rândul lor riscul la care au fost expuse datele lor personale și ce măsuri ar putea să ia pe cont propriu pentru a minimiza efectele negative (în cazul unui acces neautorizat sau al indisponibilității accesului la conturile bancare, spre exemplu).

Conținutul notificării este relativ similar cu cel prevăzut pentru notificarea transmisă către autoritatea de supraveghere (natura încălcării, date de contact ale DPO, posibile consecințe, măsuri de remediere și de diminuare a efectelor produse). În acest caz, notificarea trebuie făcută într-un limbaj clar, accesibil, simplu și în limba narativă a persoanelor vizate, fiind indicată o modalitate directă și individuală de abordare a acestora, pe diverse canale de comunicare (e-mail, SMS, dacă este posibil).

GDPR prevede trei situații, limitative, în care operatorul poate fi scutit de obligația de a notifica producerea unui incident cu risc ridicat către persoanele afectate, excepții care sunt de strictă interpretare și aplicare:

- atunci când operatorul dovedește că a pus în aplicare măsuri adecvate, tehnice și organizatorice, înainte de incident, de natură a face datele cu caracter personal (afectate de incident) neinteligibile (criptarea datelor prin metode actualizate, spre exemplu);
- atunci când operatorul demonstrează că a adoptat măsuri ulterioare pentru ca riscul să nu se materializeze;
- atunci când notificarea ar implica eforturi disproporționate, situație care trebuie, de asemenea, demonstrată de operator (spre exemplu, nu cunoaște datele de contact ale persoanelor afectate). În acest caz, este însă necesară realizarea unei informări publice, în mass-media (anunțuri vizibile și elocvente) sau pe site-ul propriu (în secțiunile relevante ale acestuia).

Cu toate acestea, este posibil ca autoritatea de supraveghere competentă să solicite operatorului să realizeze notificarea persoanelor vizate, în cazul în care acesta nu a făcut-o anterior.

ANEXA 2: ARHIVAREA DOCUMENTELOR CARE CONȚIN DATE CU CARACTER PERSONAL. MĂSURI TEHNICE ȘI ORGANIZATORICE

Recomandare generală: Documentele fizice care conțin date cu caracter personal ale salariaților (cărți de identitate, CV-uri salariați, CV-urile candidaților, fișele de post ale salariaților, certificatele de naștere ale copiilor, fișele de evaluare ale salariaților, concediile de odihnă ale salariaților, fișe ale pacienților, registre, alte documente cu caracter medical etc.) din cadrul serviciilor și departamentelor ar trebui să fie depozitate și accesate sub autoritatea Șefului de Serviciu. Departamentul X central va primi transferul altor documente de la toate celelalte servicii și/sau departamente periodic, potrivit procedurii.

> **Observație costuri**. În vedere îndeplinirii recomandării, Operatorul va analiza necesitatea achiziționării unor soluții de depozitare/arhivare electronică.

Recomandare generală: În vederea respectării principiului reducerii prelucrării datelor cu caracter personal și pentru a restrânge accesul persoanelor la datele cu caracter personal, în cazul în care biroul în care se află date este comun cu alte birouri, documentele fizice ar trebui depozitate sub cheie sub autoritatea Șefului de Serviciu sau a persoanei/persoanelor responsabile.

> **Observație costuri**. În vedere a îndeplinirii recomandării, Operatorul va analiza necesitatea achiziționării unor soluții de depozitare fizică prevăzute cu cheie.

Recomandare generală: În cadrul procedurii de lucru scrise privind protecția datelor cu caracter personal, la capitolul dedicat conlucrării între celelalte servicii și departamente și Serviciul Arhivă, va trebui inclus termenul de păstrare al documentelor cu caracter personal la celelalte servicii și departamente, modalitatea de transmitere a acestora către Serviciul Arhivă, dreptul de acces la Serviciul Arhivă.

Observație costuri. În vederea îndeplinirii recomandării, Operatorul va analiza necesitatea achiziționării unor soluții de depozitare, precum și organizarea unor spații de depozitare pentru Serviciul Arhivă.

Recomandare generală: În cazuri prelucrării electronice a unor documente care conțin date cu caracter personal, documentele fizice ar trebui scanate și stocate cu aplicație de criptare atât la nivel de document, cât și la nivel de folder de stocare, cu sprijinul Departamentului IT. Stocarea ar trebui să se facă în spații electronice de stocare, aflate la distanță. Încărcarea și în spațiul electronic de stocare și accesarea documentelor de acolo trebuie să fie făcută exclusiv prin transmisiune securizată tunelată (VPN). Tunelul peste care se realizează rețeaua virtuală trebuie să fie criptat cu cele mai stabile și sigure tehnologii bazate pe criptare cu algoritmi de tip cheie publică - cheie privată și certificate SSL de minimum 256 biți. În cadrul procedurii de lucru scrise privind protecția datelor cu caracter personal vor fi precizate termenele de stocare electronică a acestor documente, persoanele care au acces la documente, aprobările de care au nevoie pentru a accesa documentele și modul în care accesarea trebuie justificată.

Observație costuri. În vederea îndeplinirii recomandării, Operatorul va analiza necesitatea achiziționării unor soluții tehnice informatice.

Ghid GDPR pentru ONG-uri

ANEXA 3: ȘTERGEREA DATELOR CU CARACTER PERSONAL. MĂSURI TEHNICE ȘI ORGANIZATORICE

Potrivit art. 17 din Regulament aveți obligația de a șterge datele cu caracter personal în cazul în care:

- datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;
- persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea și nu există niciun alt temei juridic pentru prelucrare;
- persoana vizată se opune prelucrării și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea;
- datele cu caracter personal au fost prelucrate ilegal;
- datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale;
- datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societății informaționale în mod direct unui copil, care are mai puțin de 16 / 13 ani, nu există consimțământul acordat sau autorizat de titularul răspunderii părintești.

Regulamentul nu definește noțiunile de „*a șterge* "/„*ștergere*" - dar printr-o interpretare a definiției din Dicționarul Explicativ Român, acestea ar avea sensul de *„distrugere*". În cazul în care înregistrările aferente prelucrării datelor cu caracter personal se efectuează pe format hârtie este relativ ușor de stabilit dacă datele cu caracter personal au fost șterse sau nu, spre exemplu prin mărunțire, ardere etc. Situația poate fi mai puțin sigură în cazul în care datele cu caracter personal se stochează în format electronic, situație în care datele șterse pot să existe în continuare, într-o formă sau alta, în sistemele informatice ale organizației.

Ștergerea datelor cu caracter personal este o activitate importantă în domeniul protecției datelor cu caracter personal, având în vedere principiul potrivit căruia *„datele cu caracter personal prelucrate în orice scop/scopuri nu ar trebui păstrate mai mult decât este necesar pentru îndeplinirea acelui scop sau scopuri"*.

În unele cazuri, prin lege, se pot stabili situații în care o organizație este nevoită a șterge datele personale ale unei persoane vizate.

Ca bună practică, recomandăm ca, împreună cu operatorul, să informați clar persoanele vizate despre ce se va întâmpla cu datele lor personale, atunci când, *spre exemplu*, își închid contul, dacă acestea vor fi șterse definitiv sau pur și simplu vor fi dezactivate sau arhivate. Rețineți că, dacă arhivați datele cu caracter personal, toate normele ce reglementează protecția datelor, inclusiv dreptul de acces al persoanei vizate, rămân aplicabile.

Dacă oferiți utilizatorilor opțiunea ștergerii datelor personale încărcate de către ei înșiși, ștergerea trebuie să fie reală, adică conținutul nu ar trebui să fie recuperabil în niciun fel, de exemplu, prin accesarea unei adrese URL. Nu este recomandat să dați impresia utilizatorilor că ștergerea datelor sale personale este absolută, când de fapt nu este.

Cu siguranță, atât dumneavoastră, cât și operatorul trebuie să fiți suficienți de clari cu persoanele vizate atunci când sunt informate cu privire la ștergerea datelor și ce se întâmplă de fapt cu datele, odată șterse fiind. Trebuie contracarată în permanență problema informării persoanelor vizate cu privire la ștergerea datelor lor, când de fapt acestea au fost doar arhivate și ar putea fi repuse în uz oricând.

De asemenea, este recomandat să puneți în aplicare măsuri de protecție pentru informațiile care au fost șterse, dar care sunt, în fapt, încă în sistemele organizației.

În cazul în care operatorul a făcut publice datele cu caracter personal și este obligat să le șteargă, ținând seama de tehnologia disponibilă și de costul implementării, aceștia trebuie să ia măsuri rezonabile, inclusiv măsuri tehnice, pentru a vă informa 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, astfel încât să puteți proceda în consecință.

Important este să aveți o abordare realistă în ceea ce privește recunoașterea faptului că ștergerea informațiilor dintr-un sistem nu este întotdeauna o chestiune simplă și că este posibil, într-o primă fază, ca datele să fie scoase din uz, situație în care problema conformității cu GDPR este „suspendată” dacă:

- Datele cu caracter personal au fost șterse fără nicio intenție din partea dumneavoastră de a le utiliza sau accesa din nou, dar care ar putea să existe în continuare în sistemul electronic. De exemplu, datele ar putea aștepta să fie suprascrise cu alte date.
  - ✓ *aceste informații nu mai sunt în uz. Ca atare, problemele de respectare a normelor privind protecția datelor nu mai sunt aplicabile. (O situație paralelă ar putea fi cu deșeurile de hârtie mărunțită. Deși poate fi posibil să se reconstituie informația din bucățile de hârtie, acest lucru ar fi extrem de dificil și este puțin probabil ca organizația să aibă intenția să facă acest lucru).*

- Datele personale ar fi trebuit să fie eliminate, dar în fapt, încă sunt păstrate într-un sistem utilizat în activitatea curentă, întrucât, din motive tehnice, nu este posibilă ștergerea datelor, fără a șterge, de asemenea, alte informații deținute în același lot.
  - ✓ *în astfel de cazuri organizației care deține informațiile i se poate interzice prin lege utilizarea acestora în același mod în care utilizează datele în mod curent. Acest lucru se poate întâmpla în cazul în care o autoritate a dispus ștergerea informațiilor referitoare la o anumită persoană, dar acest lucru nu se poate fără a șterge informații despre alte persoane care sunt păstrate în același lot.*

ANEXA 4: SCHIMBUL DE DATE CU CARACTER PERSONAL. MĂSURI TEHNICE ȘI ORGANIZATORICE

Prin „schimb de date cu caracter personal” înțelegem divulgarea datelor din una sau mai multe organizații către o organizație terță parte sau mai multe sau schimbul de date între diferite entități ale unei organizații. Schimbul de date poate lua forma unui schimb de date sistematic, de rutină, caz în care are loc partajarea aceluiași set de date între aceleași organizații pentru un anume scop; schimbul de date nesistematic/ad-hoc se poate efectua în baza unor decizii de partajare a datelor, fiind nerepetitiv și care se referă doar la un număr limitat de persoane vizate.

Trebuie să cunoașteți faptul că schimbul de date poate lua una dintre următoarele forme:
- un schimb reciproc de date;
- una sau mai multe organizații furnizează date către o terță parte/terțe părți;
- mai multe organizații fac schimb de informații și le pun la dispoziția reciprocă;
- mai multe organizații fac schimb de informații și le pun la dispoziția unei terțe părți sau terțe părți;
- în mod excepțional, schimbul de date poate lua forma unei dezvăluiri care să nu aibă un caracter repetitiv, spre exemplu, în situații neprevăzute sau de urgență; sau
- părți diferite ale aceleiași organizații fac schimb de date între ele.

În practică, pot exista două tipuri principale de schimburi de date, care reprezintă prelucrări de date cu caracter personal:
- Schimbul **sistematic de date**, de rutină, în cazul în care aceleași seturi de date sunt partajate între aceleași organizații pentru un scop stabilit; acesta ar putea implica un grup de organizații care încheie un acord de schimb de date reciproc în vederea prelucrării datelor în scopuri specifice; și
- Schimbul de date **nesistematic** (nerepetitiv) sau ad-hoc, efectuat în baza unei decizii de partajare. O mare parte dintre situațiile de schimb de date au loc într-un mod pre-planificat și de rutină în baza unor norme și proceduri. Cu toate acestea, organizațiile pot

decide, de asemenea, sau pot solicita, să se efectueze o partajare a datelor în situații care nu sunt acoperite de un acord de partajare a datelor de rutină. În unele cazuri, acesta poate implica o decizie cu privire la schimbul de date, care să prevadă condițiile reale de urgență în care a fost efectuat.

Partajarea datelor cu caracter personal cu o persoană împuternicită

Deși schimbul de date are loc, în principal, între operatorii de date, situație în care ambele organizații stabilesc scopurile pentru care și modul în care sunt prelucrate datele personale, suntem în prezența unui schimb al datelor cu caracter personal și în cazul în care un operator partajează date cu o altă parte, care prelucrează date cu caracter personal în numele său. Aceste organizații sunt cunoscute sub denumirea de persoane împuternicite.

Regulamentul face o distincție între schimbul de date efectuat de către un operator de date cu alt operator, și schimbul efectuat de către un operator de date cu o persoană împuternicită. În situația în care operatorul de date prelucrează date cu caracter personal cu ajutorul unei persoane împuternicite, trebuie să se asigure că:
- există încheiat un contract încheiat între operator și persoana împuternicită de operator care vizează prelucrarea datelor cu caracter personal;
- persoana împuternicită acționează numai la instrucțiunile operatorului de date; și
- există asigurate condițiile de securitate adecvate, echivalente cu cele impuse de către operatorul de date.

Prin urmare, o persoană împuternicită implicată în schimbul de date nu are responsabilități directe de protecție a datelor; toate acestea fiindu-i impuse contractual de către operatorul de date.

Aspecte care trebuie luate în considerare:

 Ar trebui să aveți o reprezentare clară a scopului sau a setului de obiective. Având această reprezentare, veți putea ști ce date aveți nevoie să partajați și cu cine. Ca recomandare de bună practică ar fi bine să puteți demonstra această documentare.

 Nu ar trebui să partajați toate datele cu caracter personal pe care le dețineți despre cineva dacă numai anumite date sunt necesare pentru a vă atinge obiectivele. De exemplu, s-ar putea să aveți nevoie să partajați numele și adresa unei anumite persoane, nu și alte informații pe care le dețineți despre acea persoană.
 Doar organizațiile care au nevoie de datele personale ar trebui să aibă acces la datele dumneavoastră și numai personalul relevant din cadrul acestor organizații. Acest lucru ar trebui să abordeze, de asemenea, orice restricții necesare ale schimbului de date, pe mai departe, cu terțe părți.
 Ca bună practică este recomandată documentarea în acest sens, de exemplu stabilind dacă partajarea ar trebui să fie un proces continuu, de rutină sau dacă ar trebui să aibă loc ca răspuns la anumite evenimente particulare.
 Acest lucru implică abordarea securității din jurul transmiterii sau accesării datelor și stabilirea unor reguli comune de securitate.
 Pentru a verifica dacă partajarea atinge scopul preconizat, va trebui să analizați dacă este încă necesar și de a confirma că garanțiile sunt pe măsura riscurilor existente.
 Trebuie să fiți conștient de riscurile pe care le presupune partajarea datelor cu caracter personal. De exemplu, există vreo persoană care ar putea fi afectată de partajare? Există vreo persoană care ar putea obiecta? Ar putea submina încrederea persoanelor în organizațiile care dețin înregistrări ale datelor personale?
 Trebuie să analizați dacă scopul preconizat poate să fie atins fără partajarea datelor sau prin anonimizarea lor. Nu este potrivit să utilizați datele cu caracter personal pentru a planifica prestarea serviciului, de exemplu, în cazul în care acest lucru ar putea fi realizat cu informații care nu se ridică la nivelul datelor cu caracter personal.
 Trebuie să vă asigurați că partajarea este acoperită în registrul dumneavoastră de intrări.
 În situația în care datele vor fi transferate în afara UE, trebuie să vă asigurați că sunt îndeplinite obligațiile cu privire la transfer.

RGPD impune ca organizațiile să îndeplinească una sau mai multe condiţii în vederea existenței unui caracter legitim al prelucrării datelor cu caracter personal.

Consimțământul pentru prelucrarea datelor personale sensibile reprezintă una dintre condițiile Regulamentului ce oferă legitimitate pentru prelucrare, și prin urmare inclusiv pentru partajarea unor date în cadrul organizațiilor, câtă vreme acest scop este specificat expres. Regulamentul definește „acordarea consimțământului persoanei vizate" drept o: *"acțiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoștință de cauză și clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal, ca de exemplu o declarație făcută în scris, inclusiv în format electronic, sau verbal."*

Consimțământul pentru schimbul de date cu caracter personal cel mai probabil poate avea incidență în cazul:
- inexistenței unei baze legale pentru a partaja informații confidențiale sau date sensibile;
- persoanele vizate ar putea obiecta în situația partajării datelor fără consimțământul lor; sau
- în cazul în care partajarea datelor are un impact semnificativ față de persoana vizată sau față de un grup de persoane fizice.

Celelalte condiții care pot constitui temeiuri pentru schimbul de date sunt următoarele:
 executarea unui contract încheiat între dumneavoastră și persoana vizată sau pentru aplicarea unor măsuri precontractuale adoptate la cererea persoanei vizate;
 prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;
 prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;
 prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;
 prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;
 prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile

fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

În cazul în care sunt transmise date ce fac parte din categoria celor speciale, precum informații privind sănătatea unei persoane, date biometrice, date genetice sau date care dezvăluie originea rasială sau etnică a unei persoane, va trebui identificat în mod adițional față de temeiurile de mai sus una dintre cele zece temeiuri prevăzute la art. 9 alin. (2) din Regulament.

Condițiile adiționale necesare a fi îndeplinite în ceea ce privește prelucrarea, inclusiv în cazul schimbului de date cu caracter personal din categoria celor speciale sunt:

 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 Uniunii sau dreptul intern prevede ca interdicția prevăzută la alineatul (1) să nu poată fi ridicată prin consimțământul persoanei vizate;

 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, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de muncă încheiat în temeiul dreptului intern care prevede garanții adecvate pentru drepturile fundamentale și interesele persoanei vizate;

 prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul;

 prelucrarea este efectuată în cadrul activităților lor legitime și cu garanții adecvate de către o fundație, o asociație sau orice alt organism fără scop lucrativ și cu specific politic, filozofic, religios sau sindical, cu condiția ca prelucrarea să se refere numai la membri sau la foști membri ai organismului respectiv sau la persoane cu care acesta are

contacte permanente în legătură cu scopurile sale și ca datele cu caracter personal să nu fie comunicate terților fără consimțământul persoanelor vizate;

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

 prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept 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 Uniunii 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;

 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, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical și sub rezerva respectării condițiilor și garanțiilor prevăzute la alineatul (3);

 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, în temeiul dreptului Uniunii sau al dreptului intern, care prevede măsuri adecvate și specifice pentru protejarea drepturilor și libertăților persoanei vizate, în special a secretului profesional; sau

 prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), în baza dreptului Uniunii 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.

Operatorul are obligația de a informa persoanele vizate cu privire la existența unui schimb de date, inclusiv cu privire la destinatarii sau categoriile de destinatari – prin nominalizarea organizației sau tipului acesteia.

Este important ca organizațiile implicate în schimbul de date să conlucreze pentru a informa persoanele vizate cu privire la cine se află posesia datelor, cui sunt transmise acestea sau în posesia cui vor fi datele lor personale precum și scopul utilizării lor sau pentru care vor fi utilizate. Responsabilitatea principală aparține organizației care a colectat inițial datele. Cu toate acestea, ca bună practică, este recomandabil ca toate organizațiile implicate în procesul de schimb a datelor personale, să se asigure că persoanele vizate sunt și rămân conștiente în privința entității care deține datele lor personale și scopul pentru care acestea sunt prelucrate.

Ca bună practică, vă recomandăm să verificați regulile de confidențialitate ale organizației care a colectat inițial datele personale, precum și necesitatea ca aceasta să descrie categoriile de destinatari și scopul pentru care prelucrează datele cu caracter personal.

Ca bună practică, recomandăm să întreprindeți următoarele măsuri în scopul protejării informațiilor pe care le partajați cu alte organizații sau pe care alte organizații le partajează cu dumneavoastră:

• analizați ce fel de date cu caracter personal primiți de la alte organizații, asigurați-vă că știți de unde provin și orice alte condiţii ce le sunt atașate utilizării acestora;
• analizați ce fel de date partajați cu alte organizații, asigurați-vă că știți cine are acces la ele și pentru ce scopuri sunt prelucrate;
• evaluați dacă partajați date personale sensibile, asigurați-vă că asupra acestor date ați instituit un nivel de securitate mai ridicat;

• identificați cine are acces la informațiile pe care alte organizații le partajează cu dumneavoastră; ar trebui să evitați să permiteți accesul la datele care v-au fost partajate la întregul personal, în condițiile în care nu toate persoanele trebuie să le folosească pentru activitatea lor;
• conștientizați efectul pe care un incident de securitate l-ar putea avea asupra persoanelor vizate;
• conștientizați efectul pe care un incident de securitate l-ar putea avea asupra companiei, inclusiv din punctul de vedere al costurilor, al reputației sau în ceea ce privește încrederea clienților în compania dumneavoastră. Acest lucru poate fi deosebit de important în cazul în care o persoană furnizează datele sale unei organizații, dar o terță parte – destinatar pierde aceste date sau ajung să fie diseminate public.

Ar trebui să construiți o cultură în cadrul organizației dumneavoastră, astfel încât angajații să cunoască și să înțeleagă bunele practici, atât cu privire la propriile sale date, precum și în privința celor primite de la o altă organizație. Personalul ar trebui să fie conștient de politicile și procedurile de securitate și instruit în aplicarea acestora.

Măsuri de securitate fizică:

- Aveți instituit un sistem de control de calitate al accesului?
- Cum sunt monitorizați vizitatorii?
- Informațiile stocate pe hârtie sunt stocate și transferate în siguranță?
- Laptopurile și suporturile mobile (CD, memory stick) sunt blocate/încuiate pe timp de noapte?
- Dispuneți de dispozitive securizate de distrugere a hârtiei?
- Instruiți personalul în privința utilizării în siguranță a telefoanelor mobile și minimizați riscul de a le fi furate?

Măsuri de securitate tehnică:

- Aveți instituite măsuri de securitate corespunzătoare sistemului informatic utilizat, tipului de date pe care le dețineți și scopului pentru care prelucrați datele personale?

- Dacă aveți personal care lucrează de acasă, aveți instituite măsurile corespunzătoare pentru a vă asigura că nu există riscuri de compromitere a securității datelor?
- Cum este implementată și aplicată criptarea datelor?
- În ce manieră identificați cele mai obișnuite riscuri asociate utilizând un produs web? – spre exemplu, website, aplicații web sau aplicații mobile.
- Ați stabilit accesibilitate asupra datelor personale pe niveluri de cunoaștere (privilegii) și categorii de personal?
- Ce măsuri ați instituit pentru asigurarea securității tranzitului datelor cu caracter personal?

Atunci când datele cu caracter personal sunt partajate, este recomandat pentru organizația care dezvăluie datele să se asigure că acestea vor continua să fie protejate cu niveluri adecvate de securitate de către orice alte organizații care vor avea acces la acestea.

Ar trebui să vă fie clare instrucțiunile de securitate care trebuie să fie urmate atunci când schimbul de informații are loc printr-o varietate de metode, de exemplu, telefon, fax, e-mail sau fizic.

Acordurile de partajare a datelor

Acordurile de partajare a datelor - uneori cunoscute sub numele de „protocoale de partajare a datelor” - stabilesc un set comun de reguli care să fie adoptate de diferite organizații implicate într-o operațiune de schimb de date. Acestea ar putea face parte la fel de bine dintr-un contract încheiat între organizații. Ca bună practică, recomandăm încheierea unui astfel de acord/contract precum și revizuirea sa în mod regulat, în special în cazul în care informațiile sunt partajate pe scară largă, în mod regulat. Clauzele ar trebui redactate astfel încât să fie clare, concise și ușor de înțeles.

Un acord de schimb de date ar trebui să abordeze cel puțin următoarele probleme:

 scopul schimbului de date;
 potențialii destinatari ai datelor personale/categoriilor de destinatari și circumstanțele în care vor avea acces la date;
 datele care fac obiectului partajării;
 calitatea datelor partajate – acuratețe, relevanță, utilizare etc.;
 securitatea datelor;
 reținerea/stocarea datelor comune;
 temeiul legal;
 drepturile persoanelor vizate – ar trebui prevăzute proceduri în privința cererilor de acces și plângerilor. Acordul ar trebui să explice cum ar trebui să se procedeze atunci când o organizație primește o cerere de acces la datele care au făcut obiectul schimbului, precum și persoana responsabilă de asigurarea persoanei vizate a unui acces facil la toate datele partajate. În asigurarea dreptului de acces al persoanelor vizate, trebuie să furnizați informații clare despre modalitatea în care acestea pot avea acces la date, precum și instituirea unei proceduri ușoare în acest sens; trebuie să fiți capabil să localizați și să accesați datele personale pentru care sunteți responsabil, astfel încât să răspundeți în timp util persoanei solicitante;
 evaluarea perioadei, duratei/încetării acordului de partajare;
 sancțiuni pentru încălcarea acordului.

Un astfel de acord care să stea la baza schimbului de date v-ar ajuta să justificați schimbul datelor și să demonstrați că diligența dumneavoastră în ceea ce privește respectarea prevederilor RGPD.

Înainte de a intra în orice aranjament de schimb de date, ca bună practică, recomandăm să efectuați o evaluare a impactului asupra vieții private a persoanelor vizate. Acest lucru vă va ajuta să evaluați beneficiile pe care le poate aduce partajarea datelor persoanelor fizice, în special, sau societății, pe scară mai largă. Vă va ajuta, de asemenea, să identificați orice riscuri sau posibile efecte negative, cum ar fi o erodare a datelor personale, sau riscul de daune, primejdie sau jenă asupra persoanelor fizice, producerea

posibilelor daune pentru reputația organizației dumneavoastră care pot apărea în cazul în care datele sunt partajate inadecvat, sau atunci când nu sunt partajate, deși ar fi trebuit să fie.

ANEXA 5: MODEL DE PROCEDURĂ PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL

Regulile generale de protecție a datelor cu caracter personal

Întocmirea, primirea, păstrarea, accesarea, transmiterea, transportul, utilizarea și predarea documentelor care conțin date cu caracter personal se face exclusiv de către salariați instruiți cu privire la regulile de protecție a datelor cu caracter personal.

Întocmirea, primirea, păstrarea, accesarea, transmiterea, transportul, utilizarea și predarea documentelor care conțin date cu caracter personal se fac cu respectarea strică a regulilor de protecție a datelor cu caracter personal.

Întocmirea, primirea, păstrarea, accesarea, transmiterea, transportul, utilizarea și predarea documentelor care conțin date cu caracter personal se face exclusiv în scopul realizării atribuțiilor de serviciu sau îndeplinirii cerințelor legale.

Este interzisă orice divulgare a documentelor care conțin date cu caracter personal, precum și orice informație cu caracter personal cuprinsă în acestea.

***Întocmirea**. Documentele întocmite pentru salariați la nivelul serviciilor au regimul documentelor care conțin date personale și sunt supuse regulilor de protecție a datelor cu caracter personal.*

***Primirea**. Primirea documentelor care conțin date cu caracter personal se face cu promptitudine și cu îndeplinirea imediată a procedurilor de păstrare sau utilizare.*

***Păstrarea**. Documentele care conțin date cu caracter personal se păstrează în spațiu închis cu cheie, cu excepția situațiilor în care este necesară utilizarea lor firească, potrivit necesităților activității.*

***Accesarea**. Accesarea documentelor care conțin date cu caracter personal se face doar în momentul și doar câtă vreme este necesară utilizarea lor. Accesarea documentelor cu caracter personal pentru buna desfășurare a activității, precum și pentru asigurarea realizării drepturilor și intereselor clientului/furnizorilor, cumpărătorilor etc., la nivelul fiecărui serviciu, prin solicitarea acestor date de la persoana/serviciul care răspunde de ele.*

***Transmiterea**. Transmiterea documentelor fizice care conțin date personale între salariații cu atribuții în gestionarea lor se face personal sau prin curier intern special. Transportul documentelor fizice care conțin date personale se face în plic închis sau în suport închis.*

Transmiterea și transportul pe dispozitive de stocare pe suport electronic (exemplu: stick USB) a imaginilor documentelor care conțin date cu caracter personal se face respectând regulile transmiterii și transportului documentelor care conțin date cu caracter personal.

Transmiterea pe cale electronică a imaginilor documentelor care conțin date cu caracter personal se face respectând regulile de securitate informatică ale companiei.

***Utilizarea**. Documentele care conțin date cu caracter personal părăsesc spațiul în care sunt păstrate doar în intervalul de timp necesar pentru utilizarea lor firească, potrivit necesităților activității.*

***Predarea**. Predarea-primirea documentelor fizice care conțin date cu caracter personal se face cu întocmirea unui proces-verbal de predare-primire, care are același regim ca documentele care conțin date cu caracter personal.*

În cazul în care un document fizic care conține date cu caracter personal nu este reglementat în Procedura privind protecția datelor cu caracter personal, va fi înștiințat de îndată responsabilul cu protecția datelor cu caracter personal, dacă este cazul.

În cazul în care o sursă de informații care conține sau este natură să determine colectarea de date cu caracter personal nu este reglementată în Procedura privind protecția datelor cu caracter personal, va fi înștiințat de îndată responsabilul cu protecția datelor cu caracter personal, dacă acesta a fost desemnat.

Exemplu document fizic: Fișele medicale ale pacienților

Primirea. Primirea fișelor medicale se face de către salariații din cadrul Serviciului X desemnați de către șeful Serviciului X, care au fost instruiți cu privire la protecția datelor cu caracter personal și se înaintează de către fiecare salariat imediat către șeful Serviciului X.

Atenție! Fișele conțin Nume, Prenume, CNP, data nașterii, date personale privitoare la starea de sănătate precum: simptomele, diagnosticul, prescripțiile sau recomandările medicului etc.!

Păstrarea. Fișele medicale se păstrează în biroul șefului Serviciului X, cu respectarea regulilor privind păstrarea documentelor care conțin date cu caracter personal, timp de [...].

Accesarea. Accesarea spațiului de depozitare a fișelor medicale se face exclusiv de către șeful Serviciului X sau salariații special desemnați de către acesta, instruiți cu privire la protecția datelor cu caracter personal.

Utilizarea. Utilizarea fișelor medicale se face exclusiv în scopul evidențierii/înregistrării activităților medicale specifice și necesare la un moment dat, precum și pentru facilitatea corespondenței eventual necesare cu diverse autorități/instituții publice pentru clarificarea eventualelor nereguli.

Predarea. Predarea fișelor medicale se face de către șeful Serviciului X către Serviciul Y, cu respectarea regulilor privind transmiterea documentelor care conțin date cu caracter personal.

DISCLAIMER

Prezentul Ghid se bazează exclusiv pe interpretarea SSA a situațiilor prezentate, precum și a dispozițiilor legale aplicabile care pot fi, în privința problemelor menționate în acest Ghid, interpretabile, neclare sau incomplete. Recomandările noastre se bazează exclusiv pe interpretarea SSA a prevederilor legale aplicabile și a Regulamentului (UE) 2016/679 (RGPD).

Situațiile prezentate sunt cu titlu exemplificativ, motiv pentru care orice soluție în privința lor rămâne să fie dedusă pe cale de interpretare, ocazie cu care, în lipsa unei practici judiciare constante a instanțelor, soluția ce urmează a fi pronunțată de instanță este imprevizibilă.

Ghidul nu reprezintă un raport de expertiză și, prin urmare, nu este adecvat pentru utilizare și nu poate fi utilizat în niciun fel de procedură judiciară împotriva oricărei terțe persoane juridice sau fizice.

Despre SĂVESCU & ASOCIAȚII

Constituită în anul 1997, societatea civilă de avocați SĂVESCU & ASOCIAȚII s-a remarcat prin principiile și standardele sale profesionale ridicate. SSA se bucură de consilierea clienților pe plan local, cât și pe plan internațional.

Consultăm și reprezentăm cu devotament interesele clienților noștri. SSA gestionează cu ușurință, eficiență și celeritate solicitările clienților. Fiecare dosar este tratat cu seriozitate maximă, atât în ce privește fundamentarea legală, cât și în ce privește gestionarea litigiului.

Folosim toate mijloacele prevăzute de lege pentru atingerea obiectivelor clienților noștri. Practicăm avocatura din pasiune în litera și spiritul legii. Avocații SSA sunt contributori în România pentru proiectul Doing Business derulat de Banca Mondială de 10 ani, secțiunea Enforcing Contracts.

SSA își desfășoară activitatea pentru toate tipurile de clienți și pentru următoarele arii de expertiză: dreptul muncii, drept civil, drept societar, DATA PROTECTION, dreptul internetului.

De-a lungul timpului, am acordat consultanță si asistat clienți din cele mai diverse domenii, cum ar fi: conflicte de muncă, retail, jocuri de noroc, pharma, construcții, transporturi, producție de utilaje petroliere, transport aerian etc. Pe latura de litigii, SSA se bucură de succese în toate domeniile dreptului, printre care: drept penal, litigii cu profesioniști, litigii de muncă, litigii privind proprietatea intelectuală, contencios administrativ și contencios contravențional.