**COLEGIUL PSIHOLOGILOR DIN ROMÂNIA**

**ASOCIAȚIA PSIHOLOGILOR DIN ROMÂNIA**

****

**Ghid GDPR creat pentru profesia de psiholog**

|  |  |
| --- | --- |
| **Clasificarea documentului:** | Public |
| **Ref. documentului** | **GDPR-DTS-CPR-2** |
| **Versiunea:** | **1.1** |
| **Data:** | **24 May 2018** |
| **Autor:** | **Roxana Coman – Data Safety** |
| **Proprietar:** | **Colegiul Psihologilor din România și Asociația Psihologilor din România** |

Acest ghid si toate documentele aferente au fost întocmite cu suportul consultanților companiei Data Safety, care sunt specializați în GDPR, aceștia stau la dispoziția colegilor care doresc consultanță personalizată – datasafety.ro

Mulțumim mult pentru implicarea în acest proiect de mare ajutor pentru comunitatea noastră profesională!

Cuprins

[1. SFERA DE CUPRINDERE A GHIDULUI. LIMITĂRI AFERENTE 4](#_Toc514861051)

[1.1 IMPACTUL REGULAMENTULUI ASUPRA ACTIVITĂȚILOR DE PRELUCRARE 4](#_Toc514861052)

[2 Scurtă introducere asupra Regulamentului nr.679/2016 - Regulamentul General privind Protecția Datelor (GDPR) 7](#_Toc514861053)

[2.1 DOMENIUL DE APLICARE 7](#_Toc514861054)

[2.2 ASPECTE DE INTERES GDPR 8](#_Toc514861055)

[3 Calificarea formei de organizare a psihologilor din punct de vedere GDPR 11](#_Toc514861056)

[4 Temeiuri legale pentru prelucrarea datelor cu caracter personal 14](#_Toc514861057)

[4.1 Prelucrare pe bază de consimțământ (Art. 6 alin. (1) lit. (a) din Regulament) 15](#_Toc514861058)

[4.2 Prelucrare necesară pentru încheierea și executarea unui contract (Art. 6 alin. (1) lit. (b) din Regulament) 18](#_Toc514861059)

[4.3 Prelucrare necesară pentru îndeplinirea unei obligații legale (Art. 6 alin. (1) lit. (c) din Regulament) 18](#_Toc514861060)

[4.4 Prelucrare necesară pentru îndeplinirea unei sarcini care servește unui interes public (Art. 6 alin. (1) lit. (e) din Regulament) 19](#_Toc514861061)

[4.5 Prelucrare necesară în scopul unui interes legitim (Art. 6 alin. (1) lit. (f) din Regulament) 19](#_Toc514861062)

[5 Prelucrarea de categorii speciale de date 20](#_Toc514861063)

[5.1 Categorii speciale de date 20](#_Toc514861064)

[6 Informarea persoanelor vizate 22](#_Toc514861065)

[6.1 Ce conține informarea? 22](#_Toc514861066)

[6.2 Când se face informarea persoanelor? 23](#_Toc514861067)

[7 Drepturile persoanelor vizate 24](#_Toc514861068)

[7.1 Dreptul de acces al persoanei vizate 24](#_Toc514861069)

[7.2 Dreptul la rectificare a datelor cu caracter personal 25](#_Toc514861070)

[7.3 Dreptul la ștergerea datelor („dreptul de a fi uitat”) 25](#_Toc514861071)

[7.4 Dreptul la portabilitatea datelor 26](#_Toc514861072)

[7.5 Dreptul de opoziție la prelucrarea datelor 26](#_Toc514861073)

[7.6 Dreptul de a nu fi supus unor decizi automatizate, inclusiv profilarea 26](#_Toc514861074)

[7.7 Mecanisme de răspuns la cererile de exercitare a drepturilor persoanelor vizate 27](#_Toc514861075)

[7.8 Evidența gestionării cererilor de exercitare a drepturilor persoanelor vizate 27](#_Toc514861076)

[8 Evidențele operațiunilor de prelucrare a datelor cu caracter personal 29](#_Toc514861077)

[9 Responsabil cu protecția datelor 31](#_Toc514861078)

[9.1 Cazurile în care este obligatorie desemnarea unui responsabil cu protecția datelor 31](#_Toc514861079)

[9.2 Cine poate îndeplini funcția de responsabil cu protecția datelor? 33](#_Toc514861080)

[9.3 Sarcinile responsabilului cu protecția datelor sunt exemplificate de GDPR: 34](#_Toc514861081)

[10 Procesarea datelor cu caracter personal ale minorilor 35](#_Toc514861082)

[10.1 Aprecierea limitei de vârstă 35](#_Toc514861083)

[10.2 Serviciul informațional 36](#_Toc514861084)

[10.3 Consimțământul copiilor și responsabilitatea părintească 36](#_Toc514861085)

[11 Evaluarea impactului asupra protecției datelor (DPIA) 37](#_Toc514861086)

[12 Confidențialitatea și securitatea datelor 38](#_Toc514861087)

[13 Reguli specifice privind externalizarea gestiunii datelor utilizate în activitatea de zi cu zi a psihologilor utilizând servicii ale persoanelor împuternicite (servicii de cloud) 39](#_Toc514861088)

[14 Breșele de securitate 41](#_Toc514861089)

[15 Notificarea autorității de supraveghere 42](#_Toc514861090)

[16 Limitarea stocării datelor cu caracter personal 43](#_Toc514861091)

# 

# SFERA DE CUPRINDERE A GHIDULUI. LIMITĂRI AFERENTE

Prezentul Ghid se recomandă tuturor psihologilor din România și are drept scop explicitarea principalelor prevederi ale Regulamentului 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 (în continuare „Regulamentul”, “GDPR”), pentru a facilita aplicarea acestora la nivelul organelor profesiei și al formelor de exercitare a profesiei. Scopul acestui ghid este de a oferi un instrument de clarificare și interpretare a prevederilor Regulamentului, particularizat la specificul activității desfășurate de psihologi.

## IMPACTUL REGULAMENTULUI ASUPRA ACTIVITĂȚILOR DE PRELUCRARE

La un nivel general activitatea psihologilor poate fi împărțită în două mari direcții: evaluare psihologică, respectiv intervenție psihologică. Este puțin probabil ca asemenea activități să se realizeze în regim de anonimat din partea beneficiarului serviciilor psihologice și / sau fără vreo procesare scriptică sau electronică a datelor clientului. Cel mai probabil, în desfășurarea acestor activități specifice psihologii prelucrează date cu caracter personal, în diverse forme specifice: offline și online. Prin urmare, Regulamentul are un impact direct asupra activităților de prelucrare a datelor cu caracter personal.

Prelucrarea datelor cu caracter personal va trebui să se realizeze cu respectarea principiilor prevăzute în **art. 5** din *Regulament*:

* datele cu caracter personal trebuie prelucrate în mod legal, echitabil și transparent;
* datele cu caracter personal trebuie prelucrate pentru scopuri determinate, explicite și legitime;
* datele cu caracter personal trebuie să fie adecvate, relevante și neexcesive;
* datele cu caracter personal trebuie să fie exacte și actualizate;
* datele cu caracter personal trebuie să fie păstrate pe o perioadă care nu depășește perioada necesară prelucrării pentru scopul identificat;
* datele cu caracter personal trebuie să fie prelucrate într-un mod care asigură securitatea adecvată a acestora.

Toate aceste principii trebuie să guverneze fiecare activitate de prelucrare a datelor cu caracter personal.

Se impune în acest sens ca fiecare formă de organizare a profesiei să își verifice bazele de date cu caracter personal deținute în prezent pentru a concluziona dacă acestea respectă principiile enumerate de GDPR.

Ce înseamnă acest lucru pentru noi, psihologii? Va trebui să revizuim o serie de instrumente de lucru, în acord cu principiile de bună prelucrare enumerate mai sus, precum și să fim mai atenți la modul în care valorificăm, arhivăm etc. datele cu caracter personal. De exemplu, dacă am avut un client părinte, căruia i-am oferit o evaluare psihologică periodică pentru riscul profesional conducere mașina firmei, nu vom solicita în formularul cu date personale informații irelevante pentru scopul pentru care persoana a fost dispusă să ne ofere datele sale personale (ex. starea sa civilă – punctul 3 din principiile de mai sus). Cu atât mai puțin să folosim informațiile colectate cu această ocazie (ex. numărul de telefon sau adresa de e-mail) pe care mai apoi să le utilizăm în alt scop (neagreat explicit cu clientul), de exemplu pentru a-i trimite mesaje promoționale despre noul nostru curs de abilități de parenting (punctul 2 dintre principiile de mai sus). De asemenea, pentru a le putea prelucra, trebuie să obținem consimțământul său și/sau să existe un contract de prestări servicii cu compania care a trimis acest om pentru evaluare la noi, în care să se precizeze scopul și limitele între care sunt prelucrate datele cu caracter personal (punctul 1 dintre principiile de mai sus). Nici nu ar fi în regulă să dăm unor studenți voluntari să corecteze testele aplicate, fără să fi informat explicit clientul despre acest lucru (punctul 6, ultimul, din setul de principii de mai sus).

Pe scurt, va trebui să devenim conștienți de limitele în care clientul a convenit să prelucrăm datele sale personale, iar dacă dorim să le utilizăm și în alte scopuri (cu excepția cercetării sau prelucrărilor statistice), să cerem explicit consimțământul pentru fiecare scop în care dorim să le utilizăm, în limitele a ceea ce ar putea însemna un interes legitim.

Prin urmare, prevederile Regulamentului (GDPR) ar trebui citite cu atenție pentru psihologi. În cadrul acestui ghid, noi am urmărit:

1. în secțiunea 2 să explicităm câțiva termeni de bază (detaliați și în cadrul formularului general de informare și consimțire);
2. în secțiunea 3, prezentăm ce roluri / responsabilități revin celor implicați în procesarea datelor personale (operator de date, persoană împuternicită etc.) și explicăm modalitatea prin care un cabinet de psihologie poate afla care este rolul care îi revine și ce implică acest lucru;
3. în secțiunea 4, prezentăm care sunt temeiurile legale pentru care pot fi procesate date personale, cu mențiunea că dacă nu este identificat un temei legal clar pentru o asemenea prelucrare a datelor personale, aceasta este considerată ilegală;
4. în secțiunea 5, prezentăm succint diferența dintre prelucrare de date personale și prelucrarea de date personale speciale, precum și anumite aspecte care derivă din această diferențiere;
5. în secțiunea 6, prezentăm elementele care ar trebui cuprinse într-un formular de informare și când ar trebui realizată o asemenea informare de către psihologi;
6. în secțiunea 7 prezentăm drepturile persoanelor ale căror date sunt prelucrate, pentru a răspunde adecvat solicitărilor acestora;
7. în secțiunea 8, introducem ideea evidenței operațiunilor de prelucrare a datelor cu caracter personal;
8. în secțiunea 9, discutăm despre responsabilul cu protecția datelor, acea persoană despre care s-a menționat de atât de multe ori în presă, pentru a vedea în ce condiții veți avea nevoie să apelați la serviciile unui asemenea specialist;
9. în secțiunea 10 sunt prezentate aspectele ce visează preponderent prelucrarea datelor cu caracter personal ale minorilor;
10. în secțiunile 11-14 sunt prezentate o serie de aspecte ce vizează preponderent situația prelucrării online a datelor personale, precum regulile specifice privind externalizarea gestiunii datelor, breșele de securitate, evaluarea impactului asupra protecției datelor personale, deși cei mai mulți dintre psihologi, nu vor fi direct implicați în astfel de analize;
11. secțiunea 15 introduce situațiile și conținuturile care ar trebui menționate în situația în care veți notifica autoritatea de supraveghere a prelucrării datelor personale, ca urmare a unor breșe de securitate;
12. ultima secțiune, a 16-a, vizează limitele asociate stocării datelor cu caracter personal, ce pot presupune dezvoltarea unor norme interne, precum politici de arhivare, politici de ștergere.

# Scurtă introducere asupra Regulamentului nr.679/2016 - Regulamentul General privind Protecția Datelor (GDPR)

**Regulamentul (UE) 2016/679** al Parlamentului European și al Consiliului din 27 Aprilie 2016 – privind Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de aborgare a **Directivei 95/46/CE** (*Regulamentul General Privind Protecția Datelor - GDPR*) a fost adoptată la 27 aprilie 2016 și devine aplicabil de la 25 mai 2018.

Comisia Europeană a semnalat încă din anul 2012 necesitatea actualizării cadrului normativ european aplicabil în domeniul protecţiei datelor şi a propus noi reguli utilizând ca instrument normativ regulamentul.

*Regulamentul (UE) 2016/679* a intrat în vigoare pe **25 mai 2016**, iar prevederile lui vor fi aplicabile începând cu data de **25 mai 2018**.

Deşi principiile şi obiectivele principale stabilite de Directiva 95/46/CE rămân valabile, scopul principal al Regulamentului este acela de a adapta şi actualiza aceste principi în acord cu evoluţia tehnologiei.

Regulamentul stabileşte un set unic de reguli, direct aplicabile în toate statele membre ale Uniunii, destinat protejării eficiente și reale a vieţii private a persoanelor fizice de pe teritoriul Uniunii Europene.

Principiile şi regulile stabilite de Regulament pornesc de la dreptul fundamental al persoanei la protecţia datelor personale, garantat de **art. 8** al *Cartei Drepturilor Fundamentale a UE* şi **art. 16** al *Tratatului UE*.

## DOMENIUL DE APLICARE

* Regulamentul este direct aplicabil în toate statele membre UE;
* Regulamentul protejează drepturile tuturor persoanelor fizice aflate pe teritoriul UE, indiferent de situarea geografică a operatorului de date; în acest sens orice prelucrare ce vizează persoane fizice existente pe teritoriul UE (indiferent că discutăm despre domiciliu, reședință, etc), indiferent de locația de unde se face acea prelucrare, se circumscrie Regulamentului. Astfel, aplicabilitatea Regulamentului se extinde asupra tuturor entităților ce procesează date cu caracter personal ale persoanelor vizate, chiar și dacă procesarea se face din afara UE.
* extinde sfera de aplicare şi asupra operatorilor de date stabiliţi în afara UE, în măsura în care bunurile şi/sau serviciile acestora sunt adresate (şi) persoanelor aflate pe teritoriul UE.

## ASPECTE DE INTERES GDPR

Principalele noțiuni în materia procesării datelor cu caracter personal puse în discuție și folosite în GDPR sunt :

***„*GDPR”, „Regulamentul”:** REGULAMENTUL (UE) 2016/679 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor, în limba engleză General Data Protection Regulation)

***Persoana vizată:*** Orice persoană fizică care se află pe teritoriul UE;

***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;

***Împuternicit:*** înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului (*de ex. furnizori servicii IT, furnizorii servicii contabilitate și/sau /aplicații online facturare, etc*);

***Date personale:*** 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;

***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 lor respective care le revin în temeiul GDPR;

***Autoritate de supraveghere*:** înseamnă o autoritate publică independentă instituită de un stat membru în temeiul articolului 51 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;

***Restricționarea prelucrării***: înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

***Creare de profiluri*:** înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia;

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

***Sistem de evidență a datelor*:** înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice;

***Date genetice*:** înseamnă datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea persoanei respective și care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;

***Date biometrice*:** înseamnă o date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;

***Date privind sănătatea*:** înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia;

***Întreprindere*:** înseamnă o persoană fizică sau juridică ce desfășoară o activitate economică, indiferent de forma juridică a acesteia, inclusiv parteneriate sau asociații care desfășoară în mod regulat o activitate economică;

# Calificarea formei de organizare a psihologilor din punct de vedere GDPR

Regulamentul consacră regimuri juridice distincte pentru operator și persoană împuternicită sau pentru operatori asociați, caracterizate, în esență, prin faptul că:

a) Obligațiile operatorului sunt mai numeroase decât cele ale persoanei împuternicite. Obligațiile de bază în relația cu persoana vizată revin operatorului (de exemplu acesta este obligat să informeze persoanele vizate cu privire la prelucrare și caracteristicile acesteia).

b) Răspunderea operatorului și a persoanei împuternicite sunt distinct definite;

c) Relația contractuală dintre operator și persoana împuternicită trebuie să aibă la baza un contract sau orice alt acord scris;

d) Drepturile persoanelor vizate se exercită, în principal, în relația cu operatorul, persoana împuternicită având, din această perspectivă, un rol de suport pentru operator în exercitarea acestor drepturi.

Din punct de vedere GPDR este important ca fiecare entitate juridică în parte să stabilească în mod expres pentru fiecare prelucrare de date cu caracter personal felul în care aceasta se califică.

Recomandăm ca fiecare entitate juridică (formă de organizate a unui psiholog) să analizeze de la caz la caz, în funcție de rolul său în contextul fiecărei prelucrări de date cu caracter personal, dacă respectiva prelucrare se realizează în calitate de operator sau de persoană împuternicită de operator.

În calificarea psihologului ca *operator*, un rol esențial îl va avea gradul de control în ce privește respectiva prelucrare, mai concret:

a) Stabilește psihologul care vor fi persoanele vizate de prelucrare? (”*Cine?*”)

b) Stabilește psihologul ce categorii de date vor fi prelucrate? (”*Ce?*”)

c) Stabilește psihologul pentru ce scop se va realiza prelucrarea? (”*Pentru ce?*”)

d) Stabilește psihologul cum se va realiza prelucrarea? (”*Cum?*”) – de pildă, dacă se impune o prelucrate pe suport IT (aplicație) sau pe format creion-hârtie, cui se dezvăluie datele cu caracter personal, pentru cât timp se rețin datele cu caracter personal etc.

Dacă răspunsurile la întrebările de mai sus sunt majoritar ”DA”, atunci psihologul va acționa ca operator de date cu caracter personal, iar nu ca persoană împuternicită de operator.

Pe baza acestor aspecte, rezultă destul de clar faptul că psihologul are rol de operator, doar în cazul în care serviciul de psihologie este solicitat direct de către client (persoana vizată). Dacă psihologul prestează servicii psihologice în baza unui contract cu o companie, psihologul are rolul de persoană împuternicită pentru că cel puțin punctele (a) *Cine?* și (c) *Pentru ce?* de mai sus sunt stabilite de către companie.

Așadar, ar fi important de reținut următoarele situații de mai jos.:

Psihologul are rolul de operator doar dacă acționează în baza unui contract semnat între cabinet / societate civilă profesională și persoana vizată. Cu alte cuvinte, dacă serviciul este prestat la solicitarea clientului persoană fizică.

Dacă serviciile sunt prestate ca urmare a unui contract între cabinet / societate civilă profesională și o persoană juridică (o policlinică de medicina muncii, un angajator etc.), respectiv dacă serviciul este solicitat de către o persoană juridică, psihologul nu are el calitatea de operator, ci el are calitatea de persoană împuternicită. Se impune ca între psiholog și acel terț partener să existe încheiat un contract de servicii, în care să fie incluse clauzele expres menționate de GDPR, așa cum le vom individualiza în cele ce urmează.

*Conform art. 4 din Regulament:*

a) **operatorul** este persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal;

b) **persoana împuternicită de operator** este persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal pe seama operatorului.

În continuare vom face câteva precizări privind relația dintre operator și persoanele împuternicite sau între persoanele împuternicite în baza GDPR.

**Art. 28** din GDPR include regulile de bază ce reglementează relația operator / persoană împuternicită:

1. În cazul în care prelucrarea urmează să fie realizată în numele unui operator, operatorul recurge doar la persoane împuternicite care oferă garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte cerințele prevăzute în prezentul regulament și să asigure protecția drepturilor persoanei vizate.
2. Persoana împuternicită de operator nu recrutează o altă persoană împuternicită de operator fără a primi în prealabil o autorizație scrisă, specifică sau generală, din partea operatorului. În cazul unei autorizații generale scrise, persoana împuternicită de operator informează operatorul cu privire la orice modificări preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de operator, oferind astfel posibilitatea operatorului de a formula obiecții față de aceste modificări.
3. Prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un contract sau alt act juridic în temeiul dreptului Uniunii sau al dreptului intern care are caracter obligatoriu pentru persoana împuternicită de operator în raport cu operatorul și care stabilește obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate și obligațiile și drepturile operatorului. Respectivul contract sau act juridic prevede în special că persoană împuternicită de operator.
4. În cazul în care o persoană împuternicită de un operator recrutează o altă persoană împuternicită pentru efectuarea de activități de prelucrare specifice în numele operatorului, aceleași obligații privind protecția datelor prevăzute în contractul sau în alt act juridic încheiat între operator și persoana împuternicită de operator, astfel cum se prevede la alineatul (c), revin celei de a doua persoane împuternicite, prin intermediul unui contract sau al unui alt act juridic, în temeiul dreptului Uniunii sau al dreptului intern, în special furnizarea de garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să îndeplinească cerințele prezentului regulament. În cazul în care această a doua persoană împuternicită nu își respectă obligațiile privind protecția datelor, persoana împuternicită inițială rămâne pe deplin răspunzătoare față de operator în ceea ce privește îndeplinirea obligațiilor acestei a doua persoane împuternicite.
5. Aderarea persoanei împuternicite de operator la un cod de conduită aprobat, menționat la articolul 40, sau la un mecanism de certificare aprobat, menționat la articolul 42, poate fi utilizată ca element prin care să se demonstreze existența garanțiilor suficiente menționate la alineatele (1) și (4) din articolul 28 din GDPR.

# 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 din temeiurile juridice prevăzute** la **art. 6** alin. (1) din *Regulament*, respectiv:

1. Consimțământul persoanei vizate;
2. Prelucrare necesară pentru încheierea sau executarea unui contract;
3. Prelucrare necesară pentru îndeplinirea unei obligații legale;
4. Prelucrare necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;
5. Prelucrare necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;
6. Prelucrare 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:

1. 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. Acest temei juridic se va stabili în funcție de scopurile urmărite prin prelucrarea datelor cu caracter personal;
2. Alegerea temeiului juridic trebuie făcută corect de la început, deoarece schimbarea ulterioară a temeiului fără o justificare temeinică/obiectivă, fiind echivalentă cu o neconformitate;
3. Alegerea temeiului juridic trebuie documentată/susținută (cel mai frecvent, prin evidența activităților de prelucrare);
4. Persoanele vizate trebuie informate cu privire la temeiul prelucrării, ca principiu, înainte de începerea prelucrării.

În concluzie, înainte de a demara orice operațiune de prelucrare a datelor cu caracter personal se impune identificarea temeiului legal în baza căruia se face prelucrarea. Temeiul este strâns legat și va fi individualizat în funcție de modalitatea în care se solicită prestarea serviciul, prin intermediul căruia se desfășoară activitatea de prelucrare a datelor cu caracter personal.

**Ca regulă de bază operatorul este cel care are responsabilitatea de a obține consimțământul persoanei vizate**. Dacă psihologul este operator, atunci îi revine sarcina de a obține consimțământul persoanei vizate. Dacă serviciul este solicitat de către o persoană juridică, psihologul nu are responsabilitatea de a obține consimțământul persoanei vizate pentru că nu are calitatea de operator, ci el este persoană împuternicită. Dar, în acest caz, cabinetul / societate civilă profesională trebuie să se asigure contractual că partenerul obține acest consimțământ de la persoanele fizice vizate. De asemenea, în asemenea condiții psihologul trebuie să se asigure că are temeiul legal să prelucreze date personale, de exemplu prin specificarea în cadrul contractului cu operatorul sau o altă persoană împuternicită de către operator, că prelucrarea este necesară pentru executarea contractului dintre părți – temeiul al doilea în ordinea enumerării la art.6 din GDPR (în cazul nostru fiind vorba despre prestarea serviciilor de psihologie, atunci când acestea necesită prelucrarea datelor personale).

## 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 libertatea efectivă de alegere și control a prelucrării. Enumerăm mai jos câteva din cele mai importante reguli de obținere și gestionare a consimțământului:

1. **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 (e.g. căsuțe de acord pre-bifate dau doar o opțiune de dezabonare de la anumite servicii) nu reprezintă un consimțământ explicit și nu este o practică legală;
2. **Consimțământ nelegat.** Furnizarea unui serviciu solicitat de / oferit persoanei vizate nu poate fi condiționată de acordarea consimțământului pentru un alt scop, întrucât astfel, consimțământul nu ar fi liber exprimat;
3. **Consimțământ separat.** Consimțământul trebuie solicitat (i) în mod separat de termeni și condiții ori de alte documente de informare și prezentare și (ii) în mod specific pentru fiecare scop pentru care se face prelucrarea;
4. **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;
5. **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.

În acest context dacă prelucrarea datelor personale urmează a se face pentru îndeplinirea mai multor scopuri, atunci și consimțământul trebuie preluat distinct și explicit pentru fiecare scop în parte. Daca persoana fizică nu are o manifestare explicită a consimțământului, o acțiune clară de unde să rezulte consimțământul pentru scopul indicat, atunci acea prelucrare nu este legală.

De exemplu trebuie să se facă distincție între prelucrarea datelor pacienților pentru realizarea unei evaluări psihologice și prelucrarea datelor pentru un scop distinct, cum ar fi cel de marketing (transmiterea de alerte legale / newsletters prin e-mail). În acest scop persoana fizică trebuie să-si manifeste consimțământul explicit pentru fiecare scop în parte.

Ca regulă generală, o activitate de prelucrare pentru un anumit scop nu se poate baza pe mai multe temeiuri legale. Operatorul nu poate invoca mai multe temeiuri legale pentru un singur scop și nici nu poate modifica temeiurile legale comunicate persoanei vizate la momentul informării acesteia. Dacă operatorul, pe durata procesării, dorește să utilizeze datele personale în orice alt scop, diferit de cel inițial comunicat, atunci acesta are obligația de a face o nouă informare persoanei vizate, comunicând noul scop și temeiul legal corespunzător.

Poate exista în practică și situația când o persoană împuternicită dorește să prelucreze ea direct datele obținute de la persoanele vizate, dar într-un alt scop. De exemplul cabinetul psihologic ce implementează o activitate de evaluare a personalului unui client entitate juridică, dorește să folosească datele personale colectate cu ocazia evaluării pentru a transmite persoanei respective comunicări comerciale referitoare la activitatea cabinetului. În acest caz discutăm în primul rând despre modificarea calității persoanei împuternicite. Pentru această procesare în interes propriu persoana împuternicită devine operator, deoarece ea va decide când și cum va utiliza datele personale. În al doilea rând temeiul legal al procesării se modifică, fiind un consimțământ expres, iar scopul prelucrării va fi utilizarea în scop de marketing direct.

Obs:

*Participanții la operațiunea de procesare pot avea temeiuri diferite pentru același scop. În lanțul exemplificat mai sus avem chiar o astfel de situație când sunt temeiuri diferite în funcție de calitatea entității ce procesează datele, dar avem un singur scop - evaluarea.*

*În cazul în care psihologul dorește să ia acordul persoanei ce vine la testare pentru a-i transmite comunicări comerciale (alte teste etc), atunci avem alt scop, cu alta calitate a psihologului și cu alt temei legal, distinct.*

Prin urmare, operatorul care solicită consimțământul unei persoane vizate cu privire la utilizarea datelor cu caracter personal pentru mai multe scopuri, individualizând pentru fiecare scop în parte informațiile prevăzute de art.13 din GDPR.

Din cauza cerinței de a divulga temeiul legal pe care operatorul se bazează în momentul colectării datelor cu caracter personal, operatorii trebuie să decidă de la început care este baza legală aplicabilă procesării efectuate.

Obs:

*Dacă discutăm despre consimțământ, ca temei legal, atunci prin formularele de informare și acord temeiul este exprimat chiar prin textul de acord “îmi exprim acordul expres și neechivoc”. În măsura în care considerați necesar se poate include și o precizare generală de tipul: ”Temeiul legal al prelucrării este consimțământul exprimat prin prezentul acord”.*

*În cazul în care discutăm despre un angajator care își trimite salariații la testare/evaluare atunci angajatorul trebuie să includă acest temei legal în acordul care îl încheie cu salariații săi. Temeiul legal va fi diferit, în funcție de motivul ce a generat acea testare/evaluare (temei legal, consimțământ)*

## 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:

1. Există un contract valabil, pentru a cărui executare este necesară prelucrarea de date cu caracter personal; sau
2. 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:

1. Trebuie prelucrate datele unei persoane, alta decât cea cu care se încheie contractul;
2. Inițiativa încheierii contractului aparține operatorului sau unei terțe persoane.

Prelucrarea datelor cu caracter personal se poate baza pe un astfel de temei atunci când serviciile sunt prestate ca urmare a unui contract între cabinet / societate civilă profesională și o persoană juridică.

## 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 unei norme legale imperative aplicabile operatorului. 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.

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 prelucrarea mai puțin invazivă / cuprinzătoare, nu poate fi utilizat acest temei.

În exercitarea profesiei de psiholog cad sub incidența anumitor obligații legale care pot justifica anumite prelucrări de date cu caracter personal cum ar fi:

Obs:

*Un astfel de temei legal se poate individualiza, de exemplu, atunci când cabinetul/societatea profesională prelucrează datele pentru a-și îndeplini o obligație legală ce îi revine conform legislației locale sau europene (legislație specifică profesiei, legislație fiscală). Atât 4.3, cât și 4.4. se referă la acele situații posibile în care prelucrarea are loc, în absența consimțământului persoanei vizate sau a vreunui contract de executat. Sunt dificil de identificat astfel de situații (dar să presupunem situații ipotetice în care sunteți solicitați să prestați servicii psihologice pentru a preveni o catastrofă posibilă, de exemplu un potențial terorist).*

## Prelucrare necesară pentru îndeplinirea unei sarcini care servește unui interes public (Art. 6 alin. (1) lit. (e) din Regulament)

Lit. e) a alin. (1) al Art. 6 din Regulament prevede că prelucrarea se poate realiza în mod legal dacă „e) [...] *este necesară pentru îndeplinirea unei sarcini care servește unui interes public* [...];”

## Prelucrare necesară în scopul 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. Un astfel de temei legal, poate fi folosit doar în cazurile în care prelucrarea are un impact minimal asupra persoanelor vizate. Pentru o corectă fundamentare a interesului legitim, prelucrarea datelor cu caracter personal trebuie să îndeplinească următoarele caracteristici:

1. **Să vizeze un scopului legitim.** Operatorul trebuie să urmărească un interes legitim, al său ar al unui terț. Interesul legitim poate fi un interes comercial, profesional sau un scop mai larg, de exemplu un interes social.
2. **Să fie necesară.** 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.
3. **Să respecte interesele persoanei vizate.** Ca principiu, prelucrarea trebuie să fie previzibilă pentru persoana vizată și să nu creeze un prejudiciu / inconvenient persoanei vizate. Important, nu întotdeauna interesele persoanei vizate trebuie aliniate cu cele ale operatorului. Pot exista situații in care interesele operatorului pot prevala asupra celor ale persoanei vizate în cadrul unei prelucrări legitime, dar întotdeauna trebuie să existe un echilibru între interesele persoanei vizate și cele ale operatorului.

Elementul cheie legat de acest temei juridic îl reprezintă necesitatea, secondat de impactul minimal asupra persoanelor vizate. Orice alternativă mai puțin intruzivă, elimina posibilitatea utilizării acestui temei.

# Prelucrarea de categorii speciale de date

## Categorii speciale de date

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.

Concret, pentru prelucrarea adecvată a acestor categorii de date, pe lângă identificarea unui temei de prelucrare potrivit Art. 6 din Regulament, se impune implementarea unor măsuri de securitate și confidențialitate suplimentare.

De asemenea, categoriile speciale de date conferă sunt considerate ca fiind un criteriu definitoriu pentru numirea unui responsabil cu protecția datelor personale.

Sfatul nostru, pe cât posibil, ar fi să renunțați la prelucrarea unor astfel de date, dacă scopul prelucrării poate fi atins fără aceste informații. Prelucrarea unor astfel de date, necesită o serie de măsuri de securitate și confidențialitate suplimentare, de a căror monitorizare ar trebui să se ocupe o persoană desemnată special să asigure / monitorizeze protecția datelor.

În măsura în care datele referitoare la sănătatea mentală a persoanei nu pot fi evitate se recomandă verificarea încadrării prelucrării într-un context legal, cum ar fi unul din cazurile de mai jos:

1. Ca persoana vizată să își dea 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) art. 9 să nu poată fi ridicată prin consimțământul persoanei vizate
2. 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;
3. 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;
4. 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;
5. prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;
6. prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare;
7. 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;
8. 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) din Regulament;
9. 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
10. 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) din Regulament, 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.

# Informarea persoanelor vizate

Potrivit Articolelor 12-14 din Regulament, indiferent de temeiul prelucrărilor de date cu caracter personal, operatorii trebuie să se conformeze unei obligații specifice de informare a persoanelor vizate în legătură prelucrările efectuate.

Documentul de informare al persoanelor vizate cu privire la prelucrările datelor lor cu caracter personal trebuie să îndeplinească anumite cerințe formale și de conținut.

Potrivit Art. 12 alin. (1) din Regulament, informarea trebuie oferită într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu.

Documentul informare este pus la dispoziția persoanelor vizate în forme diferite, depinzând de scopurile prelucrării și de sursa datelor (persoana vizată sau altă sursă): de exemplu, politică de confidențialitate a unui website, anexă la contractul încheiat cu persoana fizică, notă de informare inserată într-un formular de aplicație pentru o poziție în cadrul operatorului, etc.

## Ce conține informarea?

Depinzând de sursa de obținere a datelor, respectiv persoana vizată însăși sau alte surse, informarea va avea un conținut specific, reglementat de Art. 13 și 14 din Regulament. Prezentăm mai jos principalele categorii de informații care trebuie furnizate persoanei vizate:

1. Identitatea și datele de contact ale operatorului și ale reprezentantului acestuia, dacă este cazul;
2. Datele de contact ale responsabilului cu protecția datelor, dacă este cazul;
3. Scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;
4. În cazul în care prelucrarea se face baza temeiului legitim, interesele legitime urmărite;
5. Categoriile de date cu caracter personal vizate;
6. Destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
7. Informații specifice privind transferurile de date personale în străinătate, dacă există o asemenea intenție;
8. Perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
9. Existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării sau a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;
10. Atunci când prelucrarea are ca temei juridic consimțământul persoanei vizate, existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;
11. Dreptul de a depune o plângere în fața autorității de supraveghere;
12. Sursa din care provin datele cu caracter personal și, dacă este cazul, dacă acestea provin din surse disponibile public;
13. 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;
14. 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.

## Când se face informarea persoanelor?

În cazul datelor cu caracter personal colectate direct de la persoana vizată, informarea se face în momentul obținerii datelor.

În cazul datelor cu caracter personal colectate din alte surse, informarea se face:

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

Indiferent dacă prelucrările de date cu caracter personal obținute de la persoana vizată sau din alte surse, informarea nu este necesară dacă și în măsura în care persoana vizată deține deja informațiile respective.

În plus, pentru cazul particular al prelucrărilor de date cu caracter personal obținute din alte surse realizate de formele de exercitare a profesiei, alte excepții de la obligația de informare pot deveni incidente:

1. în măsura în care obligația de informare este susceptibilă să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective In astfel de cazuri, operatorul ia măsuri adecvate pentru a proteja drepturile, libertățile și interesele legitime ale persoanei vizate;
2. în cazul în care datele cu caracter personal trebuie să rămână confidențiale în temeiul unei obligații legale de a păstra secretul profesional.

**Modele de informare și cerere a consimțământului persoanelor fizice** le puteți consulta în anexele prezentului ghid de informare și vă sunt puse la dispoziție de Colegiul psihologilor din România și Asociația Psihologilor din România. De menționat că prezentele anexe au caracter informativ și este necesară particularizarea fiecărui tip de document în funcție de: scopurile urmărite, identificarea operatorului, persoanele împuternicite, datele personale prelucrate ș.a.m.d.

# Drepturile persoanelor vizate

Regulamentul prevede 8 drepturi specifice în materie de prelucrare a datelor cu caracter personal, care pot fi exercitate în măsura în care nu aduc atingere drepturilor și libertăților altora:

1. Dreptul de acces la date;
2. Dreptul la rectificarea datelor;
3. Dreptul la ștergerea datelor;
4. Dreptul la restricționarea prelucrării;
5. Dreptul la portabilitatea datelor;
6. Dreptul de opoziție la prelucrarea datelor;
7. Dreptul de a nu fi supus unor decizi automatizate, inclusiv profilarea; și
8. Dreptul la notificarea destinatarilor privind rectificarea, ștergerea ori restricționarea datelor cu caracter personal.

Răspunsul la cererile persoanelor vizate trebuie să fie trimis în maximum o lună de la primirea acestora, cu posibilitatea prelungirii duratei cu maximum 2 luni, dacă vorbim despre o prelucrare complexă ori de un volum mare de astfel de cereri (în orice caz, inclusiv informarea cu privire la întârzierea unui răspuns ori refuzul de a lua măsuri trebuie transmise în termenul de 1 lună).

## Dreptul de acces al persoanei vizate

Persoana vizată are dreptul de a obține din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc și, în caz afirmativ, acces la datele respective și la următoarele informații potrivit **art 15** alin 1:

1. scopurile prelucrării;
2. categoriile de date cu caracter personal vizate;
3. 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;
4. 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;
5. 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;
6. dreptul de a depune o plângere în fața unei autorități de supraveghere;
7. în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informații disponibile privind sursa acestora;
8. existența unui proces decizional automatizat incluzând crearea de profiluri, menționat la articolul 22 alineatele (1) și (4), 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.

## Dreptul la rectificare a datelor cu caracter personal

Persoana vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc. Ținându-se seama de scopurile în care au fost prelucrate datele, persoana vizată are dreptul de a obține completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declarații suplimentare potrivit art. 16 din GDPR.

Psihologul în cazul în care este operator de date cu caracter personal are obligația legală de a opera și a corecta în cel mai scurt timp posibil toate datele inexacte (eronate sau incomplete) care privesc clienții persoane fizice.

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

Persoana vizată are dreptul de a obține din partea psihologilor ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligația de a șterge datele cu caracter personal fără întârzieri nejustificate în cazul în care se aplică unul dintre următoarele motive potrivit **art. 17** din GDPR:

1. datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;
2. persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea, în conformitate cu articolul 6 alineatul (1) litera (a) sau cu articolul 9 alineatul (2) litera (a), și nu există niciun alt temei juridic pentru prelucrarea;
3. persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (1) și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea sau persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (2);
4. datele cu caracter personal au fost prelucrate ilegal;
5. datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidența căruia se află operatorul;
6. datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societății informaționale menționate la articolul 8 alineatul (1).

În cazul în care psihologul a făcut publice datele cu caracter personal și este obligat să le șteargă este necesar ca acesta să ia măsuri rezonabile, inclusiv măsuri tehnice, pentru a informa operatorii care prelucrează datele cu caracter personal că persoana vizată a solicitat ștergerea de către acești operatori a oricăror linkuri către datele respective sau a oricăror copii sau reproduceri ale acestor date cu caracter personal.

## Dreptul la portabilitatea datelor

Dreptul la portabilitatea datelor implică obligația operatorului, de a asigura (i) furnizarea datelor primite de la persoana vizată într-un format accesibil la cererea acesteia și (ii) transmiterea unor astfel de date către alți operatori la cererea persoanei vizate, incidentă când următoarele condiții cumulative sunt îndeplinite:

1. prelucrarea se bazează pe consimțământ sau 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; și
2. este realizată prin mijloace automate (nu în formă fizică / hârtie, ci prin orice mijloace automatizate).

## Dreptul de opoziție la prelucrarea datelor

Persoanele vizate pot să se opună oricând la prelucrarea datelor lor cu caracter personal. Operatorul nu mai prelucrează datele 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.

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

În cazul în care persoana vizată se opune prelucrării în scopul marketingului direct, datele cu caracter personal nu mai sunt prelucrate în acest scop.

## Dreptul de a nu fi supus unor decizi automatizate, inclusiv profilarea

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.

Acest drept nu se aplică în care decizia:

1. este necesară pentru încheierea sau executarea unui contract între persoana vizată și un operator de date;
2. 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
3. are la bază consimțământul explicit al persoanei vizate.

## Mecanisme de răspuns la cererile de exercitare a drepturilor persoanelor vizate

Pentru a asigura tratarea cu celeritate a cererilor persoanelor vizate pentru exercitarea drepturilor specifice, respectiv a cererilor altor entități (pentru cazurile în care psihologul acționează în calitate de persoană împuternicită), următoarele mecanisme pot fi avute în vedere:

a) tratarea în timp util a cererilor persoanelor vizate;

b) redactarea unor formulare de exercitare a drepturilor / răspuns tipizate care să fie utilizate atunci când clienții / angajații / alte persoane vizate își exercită drepturile specifice;

c) Dacă cererile sunt transmise prin mijloace electronice, răspunsul trebuie transmis prin aceleași mijloace, dacă persoanele vizate nu solicită altfel;

d) Implementarea unor secțiuni specifice pentru exercitarea drepturilor persoanelor vizate online, în special în cazurile în care colectarea datelor se realizează online;

e) Pentru formele de exercitare cu personal numeros, conceperea unei proceduri specifice cu reguli clare de urmat în cazul primirii unor astfel de cereri, inclusiv cu principiile de avut în vedere în contextul conceperii răspunsurilor la cererile specifice.

## Evidența gestionării cererilor de exercitare a drepturilor persoanelor vizate

Atât când acționează ca operator cât și ca persoană împuternicită, este recomandabilă păstrarea de către psiholog a unei evidențe clare a răspunsurilor date în contextul cererilor persoanelor vizate de exercitare a drepturilor specifice în materie de prelucrare a datelor cu caracter personal, astfel:

* 1. operatorul trebuie să aibă dovezi clare scrise (inclusiv conținând răspunsurile și data transmiterii acestora) care să ateste îndeplinirea obligațiilor specifice în materie; recomandăm păstrarea evidenței pe două paliere: solicitări primite cu toate informațiile aferente cu evidențierea datei primirii acestora și respectiv răspunsuri transmise, cu evidențierea datei transmiterii răspunsurilor, iar unde este cazul de prelungire a termenului de răspuns după o lună, cu indicarea clară a motivului prelungirii.
  2. persoana împuternicită trebuie să aibă dovezi scrise care să susțină transmiterea în termen util a informațiilor solicitate respectiv implementarea în mod rezonabil a măsurilor necesare pentru conformarea cu drepturile specifice ale persoanelor vizate a operatorilor care le solicită informații / luarea de măsuri specifice.

Este preferabilă păstrarea dovezilor în formă scrisă. Cu toate acestea, dacă persoana vizată solicită anumite informații oral, este admisibilă și păstrarea unor dovezi ale înregistrărilor care să ateste răspunsul acordat unor asemenea solicitări.

# Evidențele operațiunilor de prelucrare a datelor cu caracter personal

Fiecare operator și, după caz, reprezentantul acestuia păstrează o evidență a activităților de prelucrare desfășurate sub responsabilitatea lor. Respectiva evidență cuprinde toate următoarele informații:

1. numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;
2. scopurile prelucrării;
3. descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;
4. categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale;
5. dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, în cazul transferurilor menționate la articolul 49 alineatul (1) al doilea paragraf, documentația care dovedește existența unor garanții adecvate;
6. acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;
7. acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 32 alineatul (1).

Pe de altă parte, persoana împuternicită și, după caz, reprezentantul acesteia păstrează o evidență a tuturor categoriilor de activități de prelucrare desfășurate în numele operatorului, care cuprind:

1. 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 și ale responsabilului pentru protecția datelor cu caracter personal;
2. categoriile de activități de prelucrare desfășurate în numele fiecărui operator;
3. dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, în cazul transferurilor prevăzute la articolul 49 alineatul (1) al doilea paragraf din GDPR, documentația care dovedește existența unor garanții adecvate;
4. acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate.

Conform celor precizate mai sus, un aspect obligatoriu de introdus de către toți titularii de cabinete / societăți civile profesionale de psihologie este o evidență a operațiunilor de prelucrare a datelor personale care să cuprindă toate rubricile menționate.

# Responsabil cu protecția datelor

Un element de noutate pe care acest act normativ european îl aduce în peisajul juridic românesc îl reprezintă instituirea obligativității desemnării la nivelul operatorului sau al persoanei împuternicite de operator, în anumite cazuri, a unui **responsabil cu protecția datelor**.

## Cazurile în care este obligatorie desemnarea unui responsabil cu protecția datelor

Numire unui responsabil cu protecția datelor este obligatorie conform GDPR când:

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

Autoritățile de Supraveghere locale și europene, precum si grupul de lucru dedicat interpretării și implementării GDPR au emis puncte de vedere și recomandări pentru aplicarea clauzelor GDPR.

**În ce constau ”activitățile principale”?**

Pentru a stabili activitatea principală desfășurată de un operator sau împuternicit, aceasta trebuie analizată prin raportare la operațiunile concrete de prelucrare a datelor cu caracter personal efectuate.

**La ce se referă „monitorizarea periodică și sistematică”?**

Aceasta presupune toate formele de urmărire și profilare în mediul online, inclusiv în scop de publicitate comportamentală. Activitatea de monitorizare nu este însă limitată la mediul online.

O activitate este ”periodică și sistematică” dacă este continuă și recurentă și implică în mod constant prelucrări de date cu caracter personal.

**Ce înseamnă ca o prelucrare de date cu caracter personal se realizează pe ”scară largă”?**

Pentru a se stabili dacă o prelucrare este realizată pe scară largă trebuie să se analizeze aplicabilitatea următoarelor criterii:

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

**Ce sunt ”categorii speciale de date”?**

Categoriile speciale de date sunt acelea enumerate în art.9 GDPR și cuprind date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice.

Conform art.9 alin.1 GDPR este interzisă, ca principiu, prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice.

Regula aceasta comportă însă și excepții enumerate explicit de GDPR.

**În baza acestor interpretă, în practică autoritățile au identificat câteva situații care pot constitui o monitorizare periodică și sistematică a persoanelor vizate:**

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

**Când nu este necesară desemnarea unui responsabil cu protecţia datelor?**

* atunci când nu se prelucrează pe scară largă date cu caracter personal.

**Spre exemplu:**

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

Este bine de reținut că Autoritatea de Supraveghere recomandă numirea unui responsabil cu protecția datelor, și în cazul în care numirea nu este obligatorie, întrucât o astfel de persoană este utilă operatorului pentru respectarea obligațiilor în domeniul protecției datelor cu caracter personal.

## Cine poate îndeplini funcția de responsabil cu protecția datelor?

**Art. 37 alin. 5** din **GDPR** stabilește că responsabilul cu protecția datelor trebuie să fie ”desemnat pe baza calităţilor profesionale şi, în special, a cunoştinţelor de specialitate în dreptul şi practicile din domeniul protecţiei datelor, precum şi pe baza capacităţii de a îndeplini sarcinile prevăzute la articolul 39.”

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

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

## Sarcinile responsabilului cu protecția datelor sunt exemplificate de GDPR:

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

Din nefericire la ora actuală legislația nu oferă criterii specifice care să reglementeze necesitatea angajării serviciilor de DPO. Din acest considerent nu vă putem furniza o soluție generală, ca regula de bază, soluții care să reglementeze necesitatea introducerii acestui tip de serviciu.

**Obs:**

*În contextul actual, numirea unui DPO urmează a se analiza și particulariza de la caz la caz și nu vă putem oferi un arbore decizional în acest sens.*

# Procesarea datelor cu caracter personal ale minorilor

GDPR include în art.8. reguli de protecție distincte atunci când persoana vizată este un copil.

În cazul în care se aplică articolul 6 alineatul (1) litera (a), în ceea ce privește oferirea de servicii ale societății informaționale în mod direct unui copil, prelucrarea datelor cu caracter personal ale unui copil este legală dacă copilul are cel puțin vârsta de 16 ani. Dacă copilul are sub vârsta de 16 ani, respectiva prelucrare este legală numai dacă și în măsura în care consimțământul respectiv este acordat sau autorizat de titularul răspunderii părintești asupra copilului.

Motivele pentru o protecție sporită în cazul procesării datelor personale ale copiilor sunt specificate în considerentul 38 din GDPR: "[...] *ei pot fi mai puțin conștienți de riscurile, consecințele și garanțiile în cauză și drepturile lor în ceea ce privește prelucrarea datelor cu caracter personal [...]"* Considerentul 38 de asemenea, prevede că "*O astfel de protecție specifică ar trebui să se aplice, în special, utilizării datelor cu caracter personal ale copiilor în scopul comercializării sau creării de profiluri de personalitate sau de utilizator și colectării de date cu caracter personal referitoare la copiii care utilizează serviciile oferite direct unui copil* . "Cuvintele" în special "*indică faptul că protecția specifică nu se limitează la marketing sau profilare, ci include o" colectare mai largă de date cu caracter personal în ceea ce privește copiii* ".

## Aprecierea limitei de vârstă

În comparație cu directiva actuală, GDPR creează un nivel suplimentar de protecție în cazul în care sunt prelucrate datele personale ale persoanelor fizice vulnerabile, în special ale copiilor. Articolul 8 introduce în acest sens obligații suplimentare pentru a asigura un nivel sporit de protecție a datelor cu privire la copii în legătură cu serviciile societății informaționale.

Deși GDPR stabilește limita de vârstă de 16 ani pentru obținerea legală a consimțământului direct de la un copil, el oferă flexibilitate, statele membre putând prevedea prin lege o vârstă mai mică, însă fără a coborî sub limita de 13 ani.

Cu toate acestea în legislația locală, legiuitorul face distincție între capacitatea de folosință și cea de exercițiu. În timp ce capacitatea de folosință reprezintă aptitudinea persoanei de a avea drepturi şi obligaţii civile, capacitatea de exerciţiu reprezintă aptitudinea persoanei de a încheia singură acte juridice civile și este deplină la data când persoana devine majoră, respectiv la împlinirea vârstei de 18 ani.

Din această perspectivă considerăm că, atunci când se acordă consimțământul, în ceea ce privește oferta de servicii a societății informaționale, prelucrarea datelor cu caracter personal este legală în cazul în care persoana vizată este majoră. În caz contrar, această prelucrare este legală numai dacă și în măsura în care consimțământul este acordat sau autorizat de titularul răspunderii părintești asupra minorului (copilului).

## Serviciul informațional

Un serviciu al societății informaționale înseamnă un serviciu definit conform Directivei 2015/1535: "(b)" serviciu "înseamnă orice serviciu oferit în mod obișnuit contra cost, la distanță, prin mijloace electronice și la cererea individuală a unui destinatar al serviciilor. În sensul prezentei definiții: (i) "la distanță" înseamnă că serviciul este furnizat fără prezența simultană a părților; (ii) "prin mijloace electronice" înseamnă că serviciul este trimis inițial și recepționat la destinație prin intermediul unui echipament electronic de prelucrare (inclusiv compresie digitală) și stocare a datelor și în întregime.

## Consimțământul copiilor și responsabilitatea părintească

În ceea ce privește autorizarea titularului răspunderii părintești, trebuie avut în vedere că nu întotdeauna este cazul ca titularul răspunderii părintești să fie părintele natural al copilului, iar responsabilitatea parentală să poată fi deținută de mai multe părți/persoane care pot include atât persoane juridice, cât și persoane fizice.

GDPR nu specifică modalități practice de a aduna consimțământul titularului răspunderii părintești sau de a stabili cine are dreptul să îndeplinească această acțiune. GDPR recomandă însă adoptarea unei măsuri proporționale, care să poată dovedi că operatorul a obținut consimțământul prealabil expres al persoanei ce poate dovedi că exercită în mod legal autoritatea părintească, dar totodată s-au respectat prevederile art.8 alineatul (2) și art. 5 alineatul (1c) (minimizarea datelor).

”*Operatorul depune toate eforturile rezonabile pentru a verifica în astfel de cazuri că titularul răspunderii părintești a acordat sau a autorizat consimțământul, ținând seama de tehnologiile disponibile*.”

Operatorul se poate afla în poziția de a arăta că s-au făcut eforturi rezonabile pentru a se asigura obținerea unui consimțământ valabil în legătură cu serviciile oferite unui copil și va depinde de operator să stabilească ce măsuri sunt adecvate într-un caz specific. Ca regulă generală, operatorii ar trebui să evite soluțiile de verificare care implică ele însele colectarea excesivă de date cu caracter personal.

De exemplu, în cazul în care un minor este prezentat in cabinetul unui psiholog pentru o testare/investigare/evaluare, însoțit de unul dintre părinți, psihologul poate solicita însoțitorului dovedirea calității cu o copie a certificatului de naștere a minorului.

Rămâne astfel la latitudinea operatorului de a stabili, la momentul colectării datelor cu caracter personal:

* ce măsuri de identificare a titularului răspunderii părintești aplică;
* ce date cu caracter personal colectează de la titularului răspunderii părintești;

# Evaluarea impactului asupra protecției datelor (DPIA)

Conform art. 35 para. 1 din Regulament, „*având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal. O evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare*.”

Astfel, principalele coordonate ale DPIA sunt următoarele:

a) Obligativitatea DPIA intervine atunci când prelucrarea, în special cea bazată pe noile tehnologii, este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice.

b) O evaluare unică poate fi utilizată pentru analiza unor operațiuni de procesare multiple care prezintă similitudini din perspectiva riscului generat;

c) Evaluarea trebuie realizată anterior prelucrării datelor cu caracter personal.

În analiza riscului major, relevant este și numărul persoanelor vizate.

Dacă, în urma analizei, se constată că operațiunea de procesare este susceptibilă să genereze un risc ridicat, operatorul trebuie:

1. Fie să adopte o metodologie DPIA care îndeplinește criteriile din Regulament și din ”Ghidul privind Evaluarea impactului asupra protecției datelor (DPIA) și stabilirea dacă o prelucrare este „susceptibilă să genereze un risc ridicat” în sensul Regulamentului 2016/679”8 emis de către A29 GL (”Ghidul A29 GL privind DPIA”) fie să implementeze un proces DPIA sistematic care:
2. Îndeplinește condițiile din Anexa nr. 2 din Ghidul A29 GL privind DPIA;
3. Este integrat în procesele existente de dezvoltare și revizuire operațională și de risc în conformitate cu procesele interne, contextul și cultura organizațională;
4. Implică persoanele interesate relevante și le definește atribuțiile într-un mod clar (operator, DPO, persoane vizate, persoana împuternicită etc).
5. Să transmită raportul DPIA către autoritatea de supraveghere competentă atunci când i se solicită aceasta;
6. Să consulte autoritatea de supraveghere atunci când nu au reușit să determine măsuri suficiente pentru prevenirea riscului ridicat;
7. Să revizuiască periodic DPIA și procedurile aferente:
8. Să documenteze deciziile luate.

# Confidențialitatea și securitatea datelor

Conform **art. 32** din Regulament, ”*Având în vedere stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul și persoana împuternicită de acesta implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:*

*a) pseudonimizarea și criptarea datelor cu caracter personal;*

*b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;*

*c) capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;*

*d) un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării*”.

Un rol important în evaluarea nivelului adecvat de securitate îl vor avea riscurile pe care le implică prelucrarea, riscuri ce pot fi generate, accidental ori ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

# Reguli specifice privind externalizarea gestiunii datelor utilizate în activitatea de zi cu zi a psihologilor utilizând servicii ale persoanelor împuternicite (servicii de cloud)

Specificitățile acestor proceduri și mecanisme ce presupun transferul unor date din evidența psihologilor către serverele administrate de terțe persoane (denumite generic în continuare ”prestatorii de servicii de gestiune a datelor”, persoane împuternicite în accepțiunea Regulamentului) impun o atenție sporită pentru respectarea Regulamentului și pentru evitarea oricăror breșe de securitate. De aceea, se impune luarea unor măsuri minime de siguranță:

1. Analiza tehnologiei care stă la baza infrastructurii sistemului de gestiune a datelor și îndeplinirea cerințelor de securitate impuse de GDPR etc.
2. Pentru a permite exercitarea drepturilor persoanelor vizate (”dreptul de a fi uitat”, dreptul de acces la informații, dreptul de a fi informat etc) psihologul, în calitate de operator, trebuie să se asigure că prestatorii de servicii de gestiune a datelor cunosc locația fizică a fiecărui server prin care administrează bazele de date în discuție. Aceasta se impune întrucât documentele electronice sunt mai greu de găsit decât documentele în format fizic, primele putând fi transferate prin sisteme backup, arhive sau către terțe părți/entități care s-ar putea să nu îndeplinească toate cerințele de securitate ale prezentului regulament. În scopurile respectării Regulamentului, atât operatorul cât și persoana împuternicită trebuie să aibă o evidență clară cu privire la localizarea fiecărei informații. În același scop (i.e., exercitarea drepturilor de către persoanele vizate), se impune revizuirea de către operator a protocoalelor de backup și stocare utilizate de către prestatorii de servicii de gestiune a datelor.
3. Asumarea expresă de către prestatorii de servicii de gestiune a datelor a obligațiilor ce le incumbă în temeiul Regulamentului și a legislației aplicabile în raport atât cu operatorul cât și cu persoanele vizate.
4. Determinarea locației exacte a serverelor este utilă și pentru a determina legislația aplicabilă diferitelor operațiuni.
5. Pentru a evita compromiterea datelor în integralitatea lor și a breșelor de securitate cu impact major, este recomandabilă împărțirea datelor pe diverse categorii și stocarea lor pe servere diferite.
6. Reiterarea în contractele și acordurile încheiate între operatori și prestatorii de servicii de gestiune a datelor (în calitate de persoane împuternicite) că prelucrarea datelor cu caracter personal transmise către cei din urmă se face în numele psihologilor, aceștia menținând controlul constant asupra informațiilor.
7. Crearea unor proceduri de verificare și de analiză de risc cărora să le fie supuși prestatorii de servicii de gestiune a datelor și testarea periodică a respectării legislației aplicabile în domeniul prelucrării datelor cu caracter personal (spre exemplu, dar fără a se limita la, art. 28 GDPR).
8. Verificare validității consimțământului persoanelor testate / evaluate în cazul utilizării aplicaților online puse la dispoziția psihologului de persoanele împuternicite;
9. Existența unor anexe detaliate privind măsurile minime de securitate pe care sunt obligații să le îndeplinească persoanele împuternicite ale psihologilor în cazul testărilor online.

# Breșele de securitate

Conform **art. 5** din Regulament unul din principiile de bază care guvernează prelucrarea datelor cu caracter personal este acela că datele trebuie să fie prelucrate într-un mod care asigură securitatea adecvată a acestora. Garanțiile legale ale acestui principiu se regăsesc în principal în **art. 32-34** din Regulament.

Formele de exercitare sunt obligate să implementeze măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător (**art. 32** din Regulament). Formele de exercitare trebuie să stabilească măsurile necesare și suficiente pentru a asigura securitatea datelor, pe baza criteriilor explicate în secțiunea anterioară (componenta preventivă a politicilor interne privind securitatea datelor).

Totodată, chiar dacă **art. 33** din Regulament nu o prevede în mod expres, formele de exercitare trebuie să implementeze măsuri tehnice și organizatorice care, în cazul apariției unei breșe de securitate, asigură componenta reactivă a politicilor interne privind securitatea datelor. Aceste măsuri trebuie să ajute operatorul:

* să stabilească imediat dacă s-a produs o breșă de securitate (preambul, pct. 87 din Regulament);
* dacă este cazul, să notifice autoritatea de supraveghere a prelucrării datelor cu caracter personal (art. 33 din Regulament);
* după caz, să informeze persoana sau persoanele vizate afectate de apariția breșei de securitate (art. 34 din Regulament).

Nu în ultimul rând, incidentele de securitate trebuie documentate conform **art.** **33 alin. (5)** din Regulament.

**Art. 4 alin. (12)** din Regulament definește breșa de securitate: „*o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea sau divulgarea neautorizată a datelor cu caracter personal (...) sau la accesul neautorizat la acestea*”.

În Ghidul privind notificarea încălcării securității datelor, A29 GL explică noțiunile de „distrugere”, „pierdere”, „modificare” și „divulgare neautorizată”:

1. „**distrugerea**” se referă la situația în care datele nu mai există ori nu mai există într-o formă care să le facă utilizabile de către operatori;
2. „**pierderea**” are în vedere situația în care datele pot să existe, însă operatorul a pierdut controlul sau accesul la date;
3. „**modificarea**” desemnează situația în care datele sunt corupte sau modificate în alt mod, astfel încât ele nu mai sunt complete;
4. în fine, „**divulgarea neautorizată**” are în vedere situația în care datele au fost transmise către ori accesate de către persoane neautorizate să primească sau să acceseze datele personale.

# Notificarea autorității de supraveghere

**Art. 33** din Regulament reglementează obligația operatorului de a notifica breșele de securitate către autoritatea de supraveghere a prelucrării datelor cu caracter personal. În situația în care psihologul acționează în calitate de persoană împuternicită, este obligația operatorului să notifice autoritatea de supraveghere cu privire la breșa de securitate. Totuși, psihologul, în calitate de persoană împuternicită va informa operatorul imediat ce ia cunoștință de apariția breșei de securitate.

Nu orice breșă de securitate trebuie notificată autorității de supraveghere. Conform **art. 32** din Regulament, nu este obligatorie notificarea dacă respectiva breșă nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate. Este obligația operatorului să analizeze dacă incidentul de securitate cu care se confruntă generează riscuri pentru drepturile și libertăților persoanelor vizate. Analiza se face de la caz la caz, pe baza următoarelor elemente:

* 1. tipul incidentului;
  2. natura, contextul, volumul datelor afectate;
  3. posibilitatea de a identifica persoanele vizate;
  4. consecințele incidentului asupra persoanelor vizate;
  5. consecințele incidentului asupra persoanelor vizate;
  6. circumstanțele persoanelor vizate;
  7. circumstanțele operatorului în cauză.

În cazurile în care notificarea autorității este obligatorie, aceasta trebuie făcută „fără întârziere”, de principiu nu mai târziu de 72 de ore de la data la care operatorul a luat la cunoștință de existența breșei.

Conținutul minim al notificării este reglementat de **art. 33** din Regulament.

La pregătirea notificării, psihologii vor trebui să protejeze confidențialitatea informațiilor oferite de clienți, sens în care vor oferi autorității detalii despre categoriile și numărul persoanelor afectate, fără însă a compromite confidențialitatea datelor primite de la clienți. În anumite situații, este posibil ca nu toate datele să fie de la început la dispoziția operatorului, unele amănunte devenind disponibile pe măsură ce operatorul investighează breșa. Pentru aceste situații, Regulamentul (**art. 33 alin. (4)**) și **A29 GL** recunosc posibilitatea notificării etapizate, în care operatorul transmite autorității de supraveghere datele relevante pe măsură ce acestea devin disponibile.

Informarea persoanelor vizate este obligatorie numai dacă incidentul de securitate este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor vizate. Dacă notificarea autorității de supraveghere este obligatorie ori de câte ori există un risc privind drepturile și libertățile persoanelor vizate, informarea persoanelor vizate este obligatorie atunci când există un risc ridicat pentru drepturile și libertățile acestora.

În cazurile în care informarea persoanelor vizate este obligatorie, aceasta trebuie făcută „fără întârziere”. Conținutul notificării este reglementat de **art. 34** din Regulament.

# Limitarea stocării datelor cu caracter personal

Al cincilea principiu care guvernează prelucrarea datelor cu caracter personal prevede că datele cu caracter personal trebuie să fie păstrate pe o perioadă care nu depășește perioada necesară prelucrării pentru scopul identificat.

Principiul stocării limitate a datelor cu caracter personal derivă din principiile al treilea și al patrulea:

• datele cu caracter personal trebuie să fie adecvate, relevante și neexcesive;

• datele cu caracter personal trebuie să fie exacte și actualizate.

În mod evident, datele cu caracter personal stocate pentru perioade mai lungi decât cele necesare prelucrării pentru scopul identificat vor deveni în mod automat excesive. Totodată, ele ar putea deveni nerelevate și chiar inexacte.

Regulamentul nu stabilește perioada standard de stocare a datelor cu caracter personal și nici reguli detaliate care să ajute operatorii ori persoanele împuternicite să stabilească aceasta perioadă. Revine așadar formelor de exercitare a profesiei sarcina să stabilească perioadele de reținere a datelor cu caracter personal prelucrate.

În contextul prelucrării datelor cu caracter personal, pentru a se conforma regulilor privind retenția datelor, formele de exercitare vor implementa două tipuri de reguli interne:

a) politici de arhivare, în baza cărora datele cu caracter personal care nu sunt prelucrate în activitatea curentă, dar pentru reținerea cărora există o justificare, să fie arhivate cu respectarea garanțiilor privind securitatea datelor

b) politici de ștergere, în baza cărora se vor revizui datele cu caracter personal prelucrate și se vor șterge, sau, după caz, se vor anonimiza acele date cu caracter personal de care nu mai este nevoie.

În cazul activităților profesionale, bazele de date se vor păstra pe durata impusă de legislația specifică în materie.

Dacă nu există astfel de prevederi legale sau statutare, termenul de retenție se va stabili în funcție de obiectul serviciului prestat, modalitatea și scopul în care acestea vor putea fi utilizate ( de exemplu pentru îndeplinirea obligației de plata a serviciului, baza de date se poate reține pentru o perioadă de maxim 3 ani, termenul legal generic de prescripție). În cazul în care baza de date are la baza consimțământul persoanei vizate, termenul de retenție nu poate diferi față de cel comunicat persoanei fizice la momentul obținerii consimțământului.