GHID PRIVIND EVALUAREA SISTEMELOR DE EVIDENȚĂ A DATELOR CU CARACTER PERSONAL

Evaluarea va avea ca obiect cartografierea (inventarierea) sistemelor de evidență și va ține seama de **natura**, **domeniul de aplicare**, **contextul** și **scopurile prelucrării**, precum și de **riscurile cu grade diferite de probabilitate** și **gravitate** pentru drepturile și libertățile persoanelor fizice, în scopul punerii în aplicare a măsurilor tehnice și organizatorice adecvate.

Cartografierea sistemelor de evidență a datelor trebuie să aibă în vedere, în principal, următoarele aspecte:

1. Identificarea sistemelor de evidență și a persoanelor care le administrează efectiv, atât din punct de vedere fizic cât și funcțional și legal.

În conformitate cu normele legale în materie, protecția persoanelor fizice **trebuie să se aplice** prelucrării datelor cu caracter personal prin **mijloace automatizate**, precum și **prelucrării manuale**, în cazul în care datele cu caracter personal **sunt cuprinse** sau **destinate să fie cuprinse** într-un **sistem de evidență**.

Trebuie precizat faptul că, în situația în care datele cu caracter personal nu sunt prelucrate într-un sistem de evidență sau nu sunt destinate să fie cuprinse într-un asemenea sistem, aceste date sunt protejate de dispozițiile legale existente la nivel naţional.

În acest sens, Constituţia României reglementează, în cuprinsul art.26, **dreptul la viaţă intimă, familială şi privată** ca o latură a garantării şi ocrotirii personalităţii omului, proclamată de art.1 alin.(3) ca valoare supremă, obligând **autorităţile publice la respectarea şi ocrotirea vieții intime, familială şi privată**.

De asemenea, tot Constituția României, stabilește la art.30 alin.(6) că „*libertatea de exprimare nu poate prejudicia demnitatea, onoarea, viaţa particulară a persoanei şi nici dreptul la propria imagine*”.

În același context, Codul civil român încadrează, conform art.58, **respectarea vieții private** în categoria drepturilor personalității, stabilind că orice persoană are acest drept care nu este transmisibil.

Dreptul în cauză se referă la faptul că „*orice persoană are dreptul la viaţă, la sănătate, la integritate fizică şi psihică, la demnitate, la propria imagine, la respectarea vieţii private, precum şi alte asemenea drepturi recunoscute de lege*”.

Tot Codul civil stabilește, la art.74, că pot fi considerate atingeri aduse vieţii private:

- interceptarea fără drept a unei convorbiri private, săvârşită prin orice mijloace tehnice, sau utilizarea, în cunoştinţă de cauză, a unei asemenea interceptări;
- **captarea ori utilizarea imaginii sau a vocii unei persoane aflate într-un spaţiu privat, fără acordul acesteia**;
- difuzarea de imagini care prezintă interioare ale unui spaţiu privat, fără acordul celui care îl ocupă în mod legal;
- difuzarea de ştiri, dezbateri, anchete sau de reportaje scrise ori audiovizuale privind viaţa intimă, personală sau de familie, fără acordul persoanei în cauză;
- **utilizarea, cu rea-credinţă, a numelui, imaginii, vocii sau asemănării cu o altă persoană**;
- **difuzarea sau utilizarea corespondenţei, manuscriselor ori a altor documente personale, inclusiv a datelor privind domiciliul, reşedinţa, precum şi numerele de telefon ale unei persoane sau ale membrilor familiei sale, fără acordul persoanei căreia acestea îi aparţin sau care, după caz, are dreptul de a dispune de ele**.

Sistemele de evidență analizate/cartografiate pot fi **manuale** sau **automate**, **centralizate**, **descentralizate** sau repartizate după criterii funcționale sau geografice și pot fi constituite din **baze de date în format electronic** sau **scriptic** cum ar fi sistemele informatice integrate de gestiune a datelor, “*tabele*”, “*liste*”, *documente word sau excel*, *evidenţe organizate ad-hoc*, *staţii de lucru* (individuale) ce conțin (prelucrează) date cu caracter personal, a căror existenţă este mai mult sau mai puţin necesară dar în situaţia cărora nu este conştientizată necesitatea respectării regulilor impuse de cadrul normativ în vigoare şi asupra cărora nu s-a realizat nicio evaluare.

Sistemul de evidenţă a datelor cu caracter personal este orice **set structurat** de date cu caracter personal **accesibile conform** unor **criterii specifice**, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice. (art.4 pct.6 din R.G.P.D.)

În consecință, sistemele de evidenţă a datelor cu caracter personal au următoarele caracteristici principalele:

- set – ansamblu, serie de date cu caracter personal
- structurat – care are o structură, o organizare bine definită
- accesibile – la care se ajunge uşor
- conform – funcţionează potrivit anumitor criterii
- criterii specifice – principii sau norme prestabilite pe baza cărora se face clasificarea datelor cu caracter personal şi care constituie fundamentul realizării operaţiilor de prelucrare a acestor date prin operaţiuni logice şi/sau aritmetice.

Dosarele sau seturile de dosare, precum și copertele acestora, care nu sunt structurate în conformitate cu criterii specifice, nu sunt supuse regulilor de protecție a datelor cu caracter personal deoarece nu constituie sisteme de evidență.

Sistemele de evidenţă automate a datelor cu caracter personal - **sunt sistemele în care prelucrarea datelor se efectuează prin mijloace automate.**

- Mijloacele automate fac referire la:

- introducerea codului de identificare cu ajutorul tastaturii;
- autentificarea utilizatorului prin folosirea unei parole;
- realizarea unui sistem informaţional care să refuze automat accesul unui utilizator după un anumit număr introduceri greşite ale parolei;
- accesul programatorilor la sistemele de prelucrare a datelor cu caracter personal;
- operaţiile de colectare şi introducere de date cu caracter personal într-un sistem informaţional;
- programe folosite pentru prelucrări automatizate;
- computere şi terminale de acces;
- fişier de acces, (numit log la prelucrările automate);
- implementarea unor sisteme automate de devirusare şi de securitate a sistemelor informatice;
- imprimarea datelor.

Din analiza celor prezentate mai sus se poate concluziona faptul că sistemele automate de evidenţă sunt cele care folosesc pentru activitatea de prelucrare a datelor cu caracter personal: **computerul**, **programele informatice** şi **mijloacele tehnice de imprimare**.

Sistemele de evidenţă neautomate-manuale a datelor cu caracter personal - **sunt sistemele în care prelucrarea datelor se efectuează prin alte mijloace decât cele automate, respectiv manuale.** Definiţia termenului „**manual**" dată de către D.E.X. este "**care se efectuează cu mâna**".

În scopul exemplificări prezentăm câteva sisteme de evidenţă automate sau neautomate:

- Cazierul Fiscal – operator Ministerul Finanțelor Publice;
- Registrul Naţional de Evidenţă a Persoanelor – operator Direcţia pentru Evidenţa Persoanelor şi Administrarea Bazelor de Date;
- Sistemul Informatic Unic Integrat al Asigurărilor Sociale de Sănătate (SIUI) – operator Casa Naţională de Asigurări de Sănătate;
- Evidența Nominală a Cazierului Judiciar – operator Inspectoratul General al Poliţiei Române;
- Sistemul de gestiune a dosarului în instanţă – ECRIS – operator fiecare instanță de judecată din România;
- Evidența contractelor de asigurare – operator Casa Națională de Pensii Publice.

2. Identificarea modalității prin care structura centrală ori teritorială a A.V.R. a stabilit scopul și mijloacele de prelucrare a datelor cu caracter personal: *scopurile și mijloacele prelucrării sunt stabilite în dreptul intern ori operatorul sau criteriile specifice pentru desemnarea acestuia sunt prevăzute în dreptul intern*. (ex: Legea nr.268/2021 din 9 noiembrie 2021 pentru înființarea Autorităţii Vamale Române şi pentru modificarea unor acte normative, Hotărârea nr.237/2022 din 16 februarie 2022

privind organizarea şi funcţionarea Autorităţii Vamale Române, Legea nr. 86/2006 din 10 aprilie 2006 privind Codul vamal al României, HG nr.707/2006 din 7 iunie 2006 pentru aprobarea Regulamentului de aplicare a Codului vamal al României, Legea nr. 227/2015 din 8 septembrie 2015 privind Codul fiscal, Hotărârea nr. 1/2016 din 6 ianuarie 2016 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 227/2015 privind Codul fiscal, Legea nr.207/2015 din 20 iulie 2015 privind Codul de procedură fiscală, Ordine ale Președintelui A.V.R., și altele)

Scopurile pentru care au fost constituite aceste sisteme de evidență pot fi multiple: *exercitarea atribuţiilor legale de autoritate vamală, controlul operativ, inopinat şi ulterior în domeniul vamal, supravegherea vamală, respectiv fiscală în domeniul produselor accizabile, asigurarea supravegherii şi controlului vamal la birourile vamale de frontieră şi de interior, controlul operativ şi inopinat privind prevenirea, prevenirea şi combaterea fraudei vamale şi a evaziunii fiscale, resursele umane, gestiunea economico-financiară şi administrativă, achiziţii publice, managementul resurselor umane*, *realizarea activităţii de soluţionare a petiţiilor, monitorizarea sistemelor de supraveghere video în scopul asigurării securităţii sediilor, persoanelor și bunurilor*, etc.

3. Evidențierea scopurilor în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării. [*dacă este în interesul legitim al operatorului* atunci ***ar trebui ca să nu prevaleze interesele sau drepturile și libertățile fundamentale ale persoanei vizate***, *iar temeiul juridic respectiv* ***nu ar trebui să se aplice prelucrării de către autoritățile publice în îndeplinirea sarcinilor care le revin –*** *art.6 alin.(1) lit.f din R.G.P.D.*].

Scopurile specifice în care datele cu caracter personal sunt prelucrate **ar trebui să fie explicite și legitime și să fie determinate la momentul colectării** datelor respective, iar datele cu caracter personal ar trebui prelucrate **doar dacă scopul prelucrării nu poate fi îndeplinit în mod rezonabil prin alte mijloace**.

În plan legislativ, **Legea nr.554/2004** *a contenciosului administrativ*, delimitează două caracteristici ale interesului legitim:

a) **interes legitim privat** - posibilitatea de a pretinde o anumită conduită, în considerarea realizării unui drept subiectiv viitor şi previzibil, prefigurat;

b) **interes legitim public** - interesul care vizează ordinea de drept şi democraţia constituţională, garantarea drepturilor, libertăţilor şi îndatoririlor fundamentale ale cetăţenilor, satisfacerea nevoilor comunitare, realizarea competenţei autorităţilor publice.

Definiţiile arătate pot fi exprimate printr-un singur concept şi anume că *interesul legitim este interesul persoanei fizice sau juridice care este întemeiat pe lege, fiind just*.

Acest interes legitim ar putea exista, de exemplu, atunci când există o relație relevantă și adecvată între persoana vizată și operator, cum ar fi cazul în care persoana vizată este un client al operatorului sau se află în serviciul acestuia, însă, existența unui interes legitim necesită o evaluare atentă, care să stabilească inclusiv dacă o persoană vizată poate preconiza în mod rezonabil, în momentul și în contextul colectării datelor cu caracter personal, posibilitatea prelucrării în acest scop.

De asemenea, art.6 alin.(1) lit.f din R.G.P.D., în cea de a doua teză a sa, are cuprinsă şi o clauză sine qua non ce stabileşte că realizarea interesului legitim nu trebuie să *prevaleze intereselor sau drepturilor și libertăților fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal,* ***în special atunci când persoana vizată este un copil***, iar această situație **nu se aplică** *în cazul prelucrării efectuate de autorități publice în îndeplinirea atribuțiilor lor*.

Interesele și drepturile fundamentale ale persoanei vizate ar putea prevala în special în raport cu interesul operatorului de date atunci când datele cu caracter personal sunt prelucrate în circumstanțe în care persoanele vizate nu preconizează în mod rezonabil o prelucrare ulterioară.

Un interes legitim al operatorului îl constituie prelucrarea datelor cu caracter personal, strict necesar și proporțional, în scopul:

- prevenirii fraudei vamale și fiscale, a utilizării abuzive a serviciilor sau a spălării de bani;
- asigurării securității rețelelor și a informațiilor (*de exemplu: capacitatea unei rețele sau a unui sistem de informații de a face față evenimentelor accidentale sau acțiunilor ilegale sau rău intenționate care compromit disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor cu caracter personal stocate sau transmise*);
- exercitării dreptului la libertatea de exprimare și de informare, inclusiv în mass-media și artă;

- executării drepturilor legale, inclusiv recuperarea datoriilor prin proceduri necontencioase;
- asigurării, de către o entitate, a sănătății și securității personalului său;
- monitorizării spațiilor și angajaților pentru perevenirea unor incidente la siguranța acestora.

Cu alte cuvinte, un interes legitim trebuie să fie „acceptabil în conformitate cu legea".

Temeiul juridic evidențiat la art.6 alin.(1) lit.f din R.G.P.D. are în vedere şi posibilitatea prelucrării datelor cu caracter personal fără consimţământul persoanei vizate când ***prelucrarea este necesară în scopul intereselor legitime urmărite de o parte terță***, iar în această situație operatorul care transmite datele trebuie să efectueze acest lucru în baza unei solicitări scrise, ce va conține temeiul legal, scopul prelucrării şi datele solicitate, precum şi, dacă este cazul, eventualii destinatari.

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

Operatorul **are deci obligaţia de a verifica legitimitatea solicitării**, fapt ce se poate realiza prin identificarea, în situaţia în care nu s-a făcut referire prin cererea de comunicare a datelor cu caracter personal, a documentelor legale şi atribuţiilor funcţionale ce aparţin părții terță, **fără însă a se pronunţa în legătură cu oportunitatea cererii**.

4. Categoriile de persoane vizate.

Persoană vizată este **o** persoană fizică care poate fi identificată sau identificabilă, direct sau indirect, în special prin referire la un element de identificare (art.4 pct.1 teza II-a din R.G.P.D.).

Categorii de persoane vizate: titulari ai cererilor depuse la autoritatea vamală, ai cererilor de autorizare, contribuabili, debitori, contravenienți, utilizatori ai aplicațiilor informatice, funcționari publici, beneficiari ai serviciilor publice, locale, vizitatori, pasageri, justiţiabili, contribuabili, angajaţi, membrii familiei persoanei vizate, etc.

5. Categoriile de date cu caracter personal prelucrate.

Date cu caracter personal - orice informații privind o persoană fizică identificată sau identificabilă - „ *persoana vizată* ''- (art.4 pct.1 teza I din R.G.P.D.). Ele privesc informaţiile scrise pe hârtie, precum şi informaţiile stocate în memoria unui calculator cu ajutorul unui cod binar sau stocate, de exemplu, pe un suport amovibil (CD, DVD, stik USB, etc.). Din acest punct de vedere, sunt considerate date cu caracter personal în special datele constituite din **sunete şi imagini**, în măsura în care **acestea conţin informaţii cu privire la o persoană.**

Exemple de date cu caracter personal: numele şi prenumele, sexul, data şi locul naşterii, cetăţenia, semnătura, caracteristici fizice/antropometrice; imaginile, (*de ex: cele referitoare la persoane capturate prin sisteme de supraveghere video în măsura în care persoanele pot fi identificate*); vocea (*în cazul serviciilor prin telefon, atunci când vocea clientului care oferă instrucţiuni entității care oferă serviciul este înregistrată, instrucţiunile respective înregistrate trebuie considerate ca date cu caracter personal*); telefon/fax, adresă (*domiciliu/reşedinţă*), e-mail, profesie, loc de muncă, formare profesională (*diplome – studii*), situaţie familială, situaţie militară, obişnuinţe/preferinţe/comportament; obiceiuri şi practici profesionale, date din actele de stare civilă, date din permisul de conducere/certificatul de înmatriculare, numărul dosarului de pensie, numărul asigurării sociale/asigurării de sănătate, **situaţie economică** şi **financiară**, **date privind bunurile deţinute**, **date bancare**, date de geolocalizare/date de trafic.

Datele cu caracter personal sunt date referitoare, în principiu, la ***persoanele în viaţă*** identificate sau identificabile, iar **informaţiile privind persoanele decedate nu trebuie**, în principiu, **considerate drept date cu caracter personal în temeiul R.G.P.D.**, întrucât persoana decedată nu mai reprezintă persoană fizică în conformitate cu dreptul civil.

Însă, trebuie menționat că datele cu privire la persoana decedată pot în continuare, în anumite cazuri, să beneficieze indirect de o anumită protecţie dacă operatorul de date se poate afla în situaţia de a nu putea garanta faptul că persoana la care se referă datele este încă în viaţă sau dacă a decedat ori informaţiile referitoare la persoane decedate pot face referire la persoane în viaţă.

Codul Civil român stabileşte că respectul datorat persoanei este obligatoriu şi după decesul său, cu privire la memoria sa, precum şi cu privire la corpul său iar memoria persoanei decedate este protejată în aceleaşi condiţii ca şi imaginea şi reputaţia persoanei aflate în viaţă.(art. 78 și art.79)

Normele legislative de protecție **nu se aplică** prelucrării datelor cu caracter personal care privesc **persoane juridice** și, în special, **întreprinderi cu personalitate juridică**, **inclusiv numele și tipul de persoană juridică și datele de contact ale persoanei juridice**, precum și prelucrării datelor cu caracter personal **de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice** și care, prin urmare, nu are legătură cu o activitate profesională sau comercială. Activitățile personale sau domestice ar putea include corespondența și repertoriul de adrese sau activitățile din cadrul rețelelor sociale și activitățile on-line desfășurate în contextul respectivelor activități. ***Cu toate acestea, normele de protecție se aplică operatorilor sau persoanelor împuternicite de operatori care furnizează mijloacele de prelucrare a datelor cu caracter personal pentru astfel de activități personale sau domestice.***

6. Identificarea operaţiunilor de prelucrare ce se efectuează asupra datelor cu caracter personal și a evidențelor – fișiere informatice (loguri) sau registre manuale **– privind activitățile de prelucrare aflate în responsabilitatea operatorului.**

Orice prelucrare de date cu caracter personal ar trebui să fie legală și echitabilă.

Prelucrarea datelor cu caracter personal **-** 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** (art.4 pct.2 din R.G.P.D.).

a) colectarea - strângerea, adunarea ori primirea datelor cu caracter personal prin orice mijloace legale şi din orice sursă;

b) înregistrarea - consemnarea datelor cu caracter personal într-un sistem de evidenţă automat ori neautomat, care poate fi registru, fişier automat, bază de date sau orice altă formă de evidenţă organizată, structurată ori ad-hoc sau într-un text, înşiruire de date ori document, indiferent de modalitatea în care se înscriu datele;

c) organizarea – ordonarea datelor cu caracter personal, conform unor criterii prestabilite, potrivit atribuţiilor legale ale operatorului, în scopul optimizării activităţilor de prelucrare a acestora;

d) structurarea – stocarea sistematică a datelor în așa fel încât ele să poată fi folosite în mod eficient;

e) stocarea - păstrarea pe orice fel de suport a datelor cu caracter personal culese, inclusiv prin efectuarea copiilor de siguranţă;

f) adaptarea - transformarea datelor cu caracter personal colectate iniţial, conform criteriilor prestabilite şi scopurilor pentru care au fost colectate;

g) modificarea - actualizarea, completarea, schimbarea, corectarea ori refacerea datelor cu caracter personal, în scopul menţinerii caracteristicilor de exactitate, realitate, actualitate;

h) extragerea - scoaterea unei părţi din categoria specifică de date cu caracter personal, în scopul utilizării acesteia, separat şi distinct de prelucrarea iniţială;

i) consultarea - examinarea, vizualizarea, interogarea ori cercetarea datelor cu caracter personal, fără a fi limitate la acestea, în scopul efectuării unei operaţiuni sau set de operaţiuni de prelucrare ulterioară;

j) utilizarea - folosirea datelor cu caracter personal, în tot sau în parte, de către şi în interiorul operatorului, împuterniciţilor operatorului ori destinatarului, după caz, inclusiv prin tipărire, copiere, multiplicare, scanare sau orice alte procedee similare;

k) divulgarea - a face disponibile date cu caracter personal către terţi prin transmitere, diseminare sau punerea la dispoziție în orice alt mod;

l) alinierea sau combinarea - îmbinarea, unirea sau asamblarea unor date cu caracter personal separate iniţial, într-o formă nouă, pe baza unor criterii prestabilite, pentru scopuri anume determinate;

m.) restricționarea - marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

n) ştergerea - eliminarea sau înlăturarea, în tot sau în parte, a datelor cu caracter personal din evidenţe sau înregistrări, prin împlinirea termenului de păstrare, la atingerea scopului pentru care au fost introduse, caducitatea, inexistenţa, inexactitatea;

o) distrugerea - aducerea la stare de neîntrebuinţare, în condiţiile legii, definitivă şi irecuperabilă, prin mijloace mecanice sau termice, a suportului fizic pe care au fost prelucrate date cu caracter personal.

Ținerea evidenței activităților de prelucrare de către fiecare operator este obligatorie conform art.30 din R.G.P.D. iar informațiile pe care trebuie să le cuprindă o astfel de evidență sunt următoare:

(a) *numele şi datele de contact ale operatorului***,** ale operatorului asociat şi, după caz, *ale responsabilului cu protecţia datelor*;

(b) *scopurile prelucrării*;

(c) *o descriere a categoriilor de persoane vizate şi a categoriilor de date cu caracter personal;*

(d) *categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din ţări terţe sau organizaţii internaţionale;*

(e) dacă este cazul, transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, inclusiv identificarea ţării terţe sau a organizaţiei internaţionale respective şi, în cazul transferurilor menţionate la articolul 49 alineatul (1) al doilea paragraf, documentaţia care dovedeşte existenţa unor garanţii adecvate;

(f) acolo unde este posibil, *termenele-limită preconizate pentru ştergerea diferitelor categorii de date;*

(g) acolo unde este posibil, *o descriere generală a măsurilor tehnice şi organizatorice de securitate* menţionate la articolul 32, alineatul (1).

(2) Fiecare operator şi, după caz, persoana împuternicită de operator păstrează o evidenţă *a tuturor categoriilor de activităţi de prelucrare desfăşurate în numele operatorului,* care cuprind:

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

(b) categoriile de activităţi de prelucrare desfăşurate în numele fiecărui operator;

(c) dacă este cazul, transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, inclusiv identificarea ţării terţe sau a organizaţiei internaţionale respective şi, în cazul transferurilor prevăzute la articolul 49 alineatul (1) al doilea paragraf, documentaţia care dovedeşte existenţa unor garanţii adecvate;

(d) acolo unde este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate menţionate la articolul 32 alineatul (1).

Evidenţele menţionate anterior se formulează în scris, inclusiv în format electronic iar **operatorul sau persoana împuternicită de acesta, precum şi, după caz, reprezentantul operatorului sau al persoanei împuternicite de operator pun evidenţele la dispoziţia autorităţii de supraveghere, la cererea acesteia**.

7. Stabilirea sursei de colectare a datelor cu caracter personal: direct de la persoana vizată sau indirect de la aceasta - *în mod explicit de unde*: cu ocazia realizării sarcinilor de serviciu, consultarea unor sisteme externe de evidență a datelor cu caracter personal etc.

Conform principiilor prelucrării echitabile și transparente, informațiile în legătură cu prelucrarea datelor cu caracter personal referitoare la persoana vizată *ar trebui furnizate acesteia la momentul colectării de la persoana vizată* sau, *în cazul în care datele cu caracter personal sunt obținute din altă sursă, într-o perioadă rezonabilă*, în funcție de circumstanțele cazului, *fiind necesar a se preciza care sunt consecințele unui refuz în situația în care persoana vizată are obligația de furniza date, precum și cu privire la crearea de profiluri și consecințele acesteia.*

În cazul în care datele cu caracter personal pot fi divulgate în mod legitim unui alt destinatar, **persoana vizată ar trebui informată** *atunci când datele cu caracter personal sunt divulgate pentru prima dată destinatarului*.

În cazul în care operatorul intenționează să prelucreze datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul ar trebui să furnizeze persoanei vizate, *înainte* de această prelucrare ulterioară, informații privind scopul secundar respectiv și alte informații necesare.

În cazul în care originea datelor cu caracter personal nu a putut fi comunicată persoanei vizate din cauză că au fost utilizate surse diverse, informațiile generale ar trebui furnizate.

Nu se furnizează informații în cazul în care persoana vizată **deține deja informațiile**, în cazul în care **înregistrarea** sau **divulgarea** datelor cu caracter personal **este prevăzută în mod expres de lege** sau în cazul în care **informarea** persoanei vizate se **dovedește imposibilă** sau ar **implica eforturi disproporționate**, cum ar fi atunci când prelucrarea se efectuează ***în scopuri de arhivare în interes public***, ***în scopuri de cercetare științifică*** sau ***istorică*** ori în ***scopuri statistice***, situații în care ar trebui luate în considerare numărul persoanelor vizate, vechimea datelor și orice garanții adecvate adoptate [art.13 alin.(4) coroborat cu art.14 alin.(5) din R.G.P.D.].

Informațiile transmise persoanei vizate trebuie să fie ușor accesibile și ușor de înțeles, fiind utilizat un limbaj simplu și clar, ele putând fi furnizate în combinație cu pictograme standardizate pentru a oferi într-un mod ușor vizibil, inteligibil și clar lizibil o imagine de ansamblu semnificativă asupra prelucrării avute în vedere. În cazul în care pictogramele sunt prezentate în format electronic, acestea ar trebui să poată fi citite automat.

8. Destinatarii datelor cu caracter personal atât din interiorul cât și din exteriorul operatorului de date.

Destinatar este 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.(art.4 pct.9 din R.G.P.D.)

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

Cererile de divulgare trimise de autoritățile publice trebuie să fie întotdeauna prezentate în scris, *motivate și ocazionale și nu trebuie să se refere la un sistem de evidență în totalitate sau să conducă la interconectarea sistemelor de evidență.*

Parte terță este persoana 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 (art.4 pct.10 din R.G.P.D.).

9. Dacă furnizarea de date cu caracter personal reprezintă o obligație legală ori 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.

În cazul în care prelucrarea este efectuată în conformitate cu o obligație legală a operatorului sau în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care face parte din exercitarea autorității publice, prelucrarea **ar trebui să aibă un temei în dreptul intern**, care să conțină:

- scopul prelucrării;
- condițiile generale ale cadrului normativ în materie care reglementează legalitatea prelucrării datelor cu caracter personal;
- stabilirea operatorului;
- tipul de date cu caracter personal care fac obiectul prelucrării;
- persoanele vizate;
- entitățile cărora le pot fi divulgate datele cu caracter personal;
- limitările în funcție de scop;
- perioada de stocare;
- alte măsuri pentru a garanta o prelucrare legală și echitabilă.

10. Modalitățile prin care se acordă consimțământul de către persoana vizată pentru prelucrarea datelor sale cu caracter personal: o declarație făcută în scris, inclusiv în format electronic sau verbal, bifarea unei căsuțe atunci când persoana vizitează un site, alegerea parametrilor tehnici pentru serviciile societății informaționale (ex: *consimțământul pentru prelucrarea datelor cu caracter personal de către o companie telefonică pentru a fi beneficiarul serviciului oferit de aceasta – în cauză: date de trafic*) sau orice altă declarație sau acțiune care indică în mod clar, în acest context, acceptarea de către persoana vizată a prelucrării propuse a datelor sale cu caracter personal.

Consimțământ al persoanei vizate însemnă 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 (art. 4, pct. 11 din R.G.P.D.).

- Codul civil stabileşte, la art. 1204, condiţiile pe care consimţământul trebuie să le îndeplinească pentru a fi valabil, şi anume: **să fie serios, liber şi exprimat în cunoştinţă de cauză.**
- Art. 1206, alin. (1) din acelaşi cod, precizează care sunt viciile consimţământului: **când este dat din eroare, surprins prin dol -** *eroare provocată de manopere frauduloase* **- sau smuls prin violenţă** ori **în caz de leziune** (alin.2 al aceluiași articol).

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

O atenție deosebită trebuie acordată copiilor deoarece ei au nevoie de o protecție specifică a datelor lor cu caracter personal, întrucât pot fi mai puțin conștienți de riscurile, consecințele, garanțiile în cauză și drepturile lor în ceea ce privește prelucrarea datelor cu caracter personal.

11. Dacă a fost desemnat responsabilul cu protecţia datelor personal, experiența în domeniu, sarcinile acestuia și dacă ele sunt inserate în fișa postului.

Responsabil cu protecția datelor este persoana desemnată din cadrul operatorului sau a persoanei împuternicite ori în baza unui contract de servicii ce **monitorizează și evaluează conformitatea** cu normele de drept al Uniunii sau drept intern, referitoare la protecția datelor cu caracter personal și care ***este implicat,*** de către operator și persoana împuternicită de operator, ***în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal*** (art.37 – art.39 din R.G.P.D.).

12. Identificarea utilizatorilor și a operațiunilor de prelucrare date în competența acestora.

Dacă s-a realizat instruirea utilizatorilor în domeniul prelucrării datelor cu caracter personal.

Utilizator este persoana care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, este autorizată să prelucreze date cu caracter personal (art.4 pct.10 teza II-a din R.G.P.D.) și, în consecință, acesta trebuie să aibă inserate în fișa postului atribuțiile referitoare la **prelucrarea datelor cu caracter personal.**

De asemenea, este necesar ca utilizatorii de date cu caracter personal să dea o declarație de confidențialitate referitoare la prelucrarea datelor cu caracter personal, document ce poate fi completat doar o singură dată pentru toate sistemele de evidență la care au acces, dar care poate fi completat și în mai multe exemplare atunci când sistemele în cauză aparțin unor operatori externi structurii din care fac parte aceștia și numai dacă opeartorii respectivi solicită acest fapt.

13. Transferurile de date în state terțe, iar în situația în care se realizează, trebuie stabilite următoarele:

- temeiul juridic;
- categoria de date cu caracter personal;
- modalitățile de transfer.

14. Termenele de păstrare a datelor cu caracter personal, fiind necesar ca perioada pentru care datele cu caracter personal sunt stocate să fie limitată strict la minimum.

În vederea asigurării faptului că datele cu caracter personal, din cadrul unor sisteme de evidență proprii, nu sunt păstrate mai mult timp decât este necesar, ar trebui să se stabilească de către operator termene pentru ștergere sau revizuirea periodică și ar trebui să fie luate toate măsurile rezonabile pentru a se asigura că datele cu caracter personal care sunt inexacte sunt rectificate sau șterse.

15. Dacă există vreun proces decizional automatizat, incluzând crearea de profiluri, și care stă la baza unor decizii ce produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă, (*de exemplu: refuzul automat al unei cereri de credit on-line sau practicile de recrutare pe cale electronică, fără intervenție umană*), trebuie relevate informații privind logica utilizată, precum importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată**.**

Crearea de profiluri trebuie realizată:

- prin utilizarea unor proceduri matematice sau statistice adecvate;
- prin implementarea măsurilor tehnice și organizatorice care să asigure că factorii ce duc la inexactități ale datelor cu caracter personal sunt corectați și că riscul de erori este redus la minimum;
- prin securizarea datelor cu caracter personal într-un mod care să țină seama de pericolele potențiale la adresa intereselor și drepturilor persoanei vizate;
- prin prevenirea efectelor discriminatorii împotriva persoanelor pe motiv de rasă sau origine etnică, opinii politice, religie sau convingeri, apartenență sindicală, caracteristici genetice, stare de sănătate sau orientare sexuală sau care să ducă la măsuri care să aibă asemenea efecte;
- numai în condiții specifice atunci când privește categorii speciale de date cu caracter personal.

16. Măsurile tehnice şi organizatorice dispuse pentru protecția datelor cu caracter personal.

Datele cu caracter personal trebuie prelucrate într-un mod care să asigure în mod adecvat **securitatea** și **confidențialitatea** acestora, inclusiv în scopul prevenirii accesului neautorizat la acestea sau utilizarea neautorizată a datelor cu caracter personal și a echipamentului utilizat pentru prelucrare, iar măsurile aplicate trebuie să respecte, în special, principiul protecției datelor începând cu momentul conceperii și cel al protecției implicite a datelor (*de exemplu: pseudonimizarea, criptarea, transparența în ceea ce privește funcțiile și prelucrarea datelor cu caracter personal, abilitarea persoanei vizate să monitorizeze prelucrarea datelor, abilitarea operatorului să creeze elemente de siguranță și să le îmbunătățească*).

17. Dacă au fost afișate drepturile persoanei vizate, conferite de lege, în spaţiile accesibile publicului ori pe pagina de internet.

Informațiile care se adresează publicului sau persoanei vizate trebuie să fie concise, ușor accesibile și ușor de înțeles și să se utilizeze un limbaj simplu și clar, precum și vizualizare acolo unde este cazul. Ele pot fi furnizate în format electronic, de exemplu atunci când sunt adresate publicului, prin intermediul unui site, în special în situații în care datorită multitudinii actorilor și a complexității, din punct de vedere tehnologic, a practicii, este dificil ca persoana vizată să știe și să înțeleagă dacă datele cu caracter personal care o privesc sunt colectate, de către cine și în ce scop, cum este cazul publicității on-line.

Întrucât copiii necesită o protecție specifică, orice informații și orice comunicare, în cazul în care prelucrarea vizează un copil, trebuie să fie exprimate într-un limbaj simplu și clar, astfel încât copilul să îl poată înțelege cu ușurință.

18. Câte solicitări au fost primite din partea persoanelor vizate în exercitarea drepturilor conferite de lege și modalitățile de soluționare. Care sunt măsurile pentru a verifica identitatea unei persoane vizate care solicită acces la date, în special în contextul serviciilor on-line și al identificatorilor online? (*operatorul nu ar trebui să rețină datele cu caracter personal în scopul exclusiv de a fi în măsură să reacționeze la cereri potențiale*).

Operatorul trebuie să prevadă modalități de facilitare a exercitării de către persoana vizată a drepturilor care îi sunt conferite de lege, inclusiv mecanismele prin care aceasta poate solicita și, dacă este cazul, obține, în mod gratuit, în special, acces la datele cu caracter personal, precum și rectificarea sau ștergerea acestora și exercitarea dreptului la opoziție.

Operatorul trebuie să ofere, de asemenea, modalități de introducere a cererilor pe cale electronică, mai ales în cazul în care datele cu caracter personal sunt prelucrate prin mijloace electronice.

Operatorul are obligația de a răspunde cererilor persoanelor vizate fără întârzieri nejustificate și cel târziu în termen de o lună și, în cazul în care nu intenționează să se conformeze respectivele cereri, să motiveze acest refuz.

19. Controale efectuate de autoritatea națională de supraveghere a protecției datelor. Măsuri dispuse ori sancțiuni aplicate.

Autoritatea de supraveghere este o autoritate publică independentă instituită de un stat membru în temeiul articolului 51 din R.G.P.D, ea fiind responsabilă de monitorizarea aplicării regulamentului, în vederea protejării drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea și în vederea facilitării liberei circulații a datelor cu caracter personal în cadrul U.E. (art. 4, pct. 21, coroborat cu art. 51 din R.G.P.D.) – în România este Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

20. Incidente de securitate în domeniul protecției datelor cu caracter personal. Măsurile de remediere luate și care au fost consecințele asupra persoanei vizate.

Încălcarea securității datelor cu caracter personal este o încălcare a securității care duce, în mod accidental sau ilegal, la **distrugerea, pierderea, modificarea**, sau **divulgarea neautorizată** a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la **accesul neautorizat** la acestea (art.4 pct.12 din R.G.P.D.).

Operatorul **trebuie să notifice autoritatea de supraveghere de îndată ce a luat cunoștință** de producerea unei încălcări a securității datelor cu caracter personal, **fără întârziere nejustificată** și, dacă este posibil, **în cel mult 72 de ore după ce a luat la cunoștință** de existența acesteia, cu excepția cazului în care operatorul este în măsură să demonstreze, în conformitate cu principiul responsabilității, că încălcarea securității datelor cu caracter personal nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice.

Atunci când notificarea nu se poate realiza în termen de 72 de ore, aceasta trebuie să cuprindă motivele întârzierii, iar informațiile pot fi furnizate treptat, fără altă întârziere.

De asemenea, operatorul **trebuie să comunice persoanei vizate o încălcare a securității** datelor cu caracter personal, fără întârzieri nejustificate, **în cel mai scurt timp posibil în mod rezonabil** și în strânsă cooperare cu autoritatea de supraveghere, atunci când încălcarea este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanei fizice, pentru a-i permite să ia măsurile de precauție necesare iar comunicarea va descrie natura încălcării securității datelor cu caracter personal și va cuprinde recomandări pentru persoana fizică în cauză în scopul atenuării eventualelor efecte negative.

De exemplu, necesitatea de a atenua un risc imediat de producere a unui prejudiciu ar presupune comunicarea cu promptitudine către persoanele vizate, în timp ce necesitatea de a implementa măsuri corespunzătoare împotriva încălcării în continuare a securității datelor cu caracter personal sau împotriva unor încălcări similare ale securității datelor cu caracter personal ar putea justifica un termen mai îndelungat pentru comunicare.

21. Încheierea operațiunilor de prelucrare și destinația ulterioară a datelor:

- **prelucrare ulterioară într-un alt scop decât cel pentru care acestea au fost obținute, cu sau fără consimțământul persoanei vizate** (*ar trebui să fie permisă doar atunci când prelucrarea este compatibilă cu scopurile respective pentru care datele cu caracter personal au fost inițial colectate – prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice ar trebui considerată ca reprezentând operațiuni de prelucrare legale compatibile*);
- ștergere, distrugere, arhivare;
- transformare în date anonime și stocate exclusiv în scopuri statistice, de cercetare istorică sau științifică;
- transferare unui alt operator.

Pentru a stabili dacă scopul prelucrării ulterioare este compatibil cu scopul pentru care au fost colectate inițial datele cu caracter personal, operatorul, după ce a îndeplinit toate cerințele privind legalitatea prelucrării inițiale, ar trebui să țină seama, printre altele, de orice legătură între respectivele scopuri și scopurile prelucrării ulterioare preconizate, de contextul în care au fost colectate datele cu caracter personal, în special de așteptările rezonabile ale persoanelor vizate, bazate pe relația lor cu operatorul, în ceea ce privește utilizarea ulterioară a datelor, de natura datelor cu caracter personal, de consecințele prelucrării ulterioare preconizate asupra persoanelor vizate, precum și de existența garanțiilor corespunzătoare atât în cadrul operațiunilor de prelucrare inițiale, cât și în cadrul operațiunilor de prelucrare ulterioare preconizate.

22. Motivarea necesității păstrării sistemelor proprii existente, a realizării operațiunilor de prelucrare, precum și a numărului de utilizatori ce au acces la sistemele de evidență a datelor cu caracter personal.

23. Dificultăţi întâmpinate în aplicarea cadrului legislativ.

24. Propuneri pentru îmbunătățirea activități în domeniul de referință.