CAMERA NAȚIONALĂ A CONSILIERILOR ÎN PROPRIETATE INDUSTRIALĂ DIN ROMÂNIA

06 august 2018

GHID DE BUNE PRACTICI

CONSILIERUL ÎN PROPRIETATE INDUSTRIALĂ SI REGULAMENTUL GENERAL PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL

http://patent-chamber.ro/

I. ASPECTE GENERALE

A. NOTĂ INTRODUCTIVĂ

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" sau "GDPR") produce efecte în mod direct în toate cele 28 state membre ale Uniunii Europene începând cu data de 25 mai 2018.

La nivel național, printre altele, în legătură cu GDPR, trebuie avute în vedere și Legea 129/2018 pentru modificarea și completarea Legii nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum și pentru abrogarea Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date precum și Legea 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

Autoritatea de supraveghere la nivel național, în România, este Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal ("ANSPDCP"), ce are următoarele date de contact:

Adresa: B-dul G-ral. Gheorghe Magheru, Nr. 28-30
Sector 1, cod postal 010336
București,
România,

Website: http://www.dataprotection.ro.

Având în vedere că, în desfășurarea activității lor specifice, consilierii în proprietate industrială, indiferent de forma de desfășurare a activității, cabinete individuale autorizate, cabinete individuale asociate pe baza de contract, societăți civile profesionale persoane juridice sau în societăți comerciale având ca unic obiect activitățile in domeniul proprietății industriale, prelucrează date cu caracter personal, GDPR este incident acestora.

În acest sens, Camera Națională a Consilierilor în Proprietate Industrială din România („CNCPIR") a adoptat prezentul Ghid de bune practici pentru a explicita principalele obligații ce incumbă consilierilor în proprietate industrială cu privire la prelucrarea datelor cu caracter personal în cadrul activității acestora.

B. GLOSAR

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

- „**prelucrare**”: 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;

- „**creare de profiluri**”: 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**”: 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;

- „**operator**”: persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;

- „**persoană împuternicită de operator**”: persoana fizică sau juridică, autoritatea

publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

- „**destinatar**”: persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. 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**”: 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: 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**”: 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;

- „**reguli corporatiste obligatorii**”: 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;

- „**prelucrare transfrontalieră**”:

a. fie prelucrarea datelor cu caracter personal care are loc în contextul activităților sediilor din mai multe state membre ale unui operator sau ale unei persoane împuternicite de operator pe teritoriul Uniunii, dacă operatorul sau persoana împuternicită de operator are sedii în cel puțin două state membre; sau

b. fie prelucrarea datelor cu caracter personal care are loc în contextul activităților unui singur sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, dar care afectează în mod semnificativ sau este susceptibilă de a afecta în mod semnificativ persoane vizate din cel puțin două state membre.

- **Comitetul european pentru protecția datelor**: organ al Uniunii Europene cu personalitate juridică alcătuit din șeful unei autorități de supraveghere din fiecare stat membru și din Autoritatea Europeană pentru Protecția Datelor sau reprezentanții respectivi ai acestora, ce asigură aplicarea coerentă a GDPR și care a înlocuit începând cu 25 mai 2018 Grupul de lucru Articolul 29 (WP29).

- **Consilier în proprietate industrială**: persoana fizică atestată în condițiile Ordonanței Guvernului nr. 66/2000 privind organizarea și exercitarea profesiei de consilier în proprietate industrială și înscrisă în Registrul național al consilierilor în proprietate industrială.

II. CALIFICAREA CONSILIERULUI ÎN PROPRIETATE INDUSTRIALĂ DIN PERSPECTIVA GDPR

Conform articolului 4 din GDPR **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**, în timp ce **persoana împuternicită** este persoana fizică sau juridică, autoritatea publică, agenția sau alt organism **care prelucrează datele cu caracter personal în numele operatorului.**

Regimul juridic aplicabil unui operator de date cu caracter personal este diferit de cel al unei persoane împuternicite.

În esență, obligațiile operatorului sunt mai numeroase decât cele ale unei persoane împuternicite, iar drepturile persoanelor vizate se exercită, în principal, în relația cu operatorul, persoana împuternicită având rol de asistare a operatorului în exercitarea acestor drepturi.

Este esențial pentru consilierul în proprietate industrială să califice în mod corect calitatea sa pentru fiecare prelucrare de date cu caracter personal, inclusiv în raport cu terții cu care contractează în legătură cu diverse servicii (ex. societăți care emit bonuri de masă pentru salariații săi; societăți de IT cu care contractează pentru a-i fi furnizate servicii de cloud, găzduire website, etc; societăți care asigură pază și protecție locații; societăți care asigură servicii de turism; societăți care furnizează accesul la platforme legislative; societăți care prestează servicii de traduceri, expertize, etc).

În raport de clienții săi, consilierul în proprietate industrială prestează un serviciu, dar aceasta nu îl califică ca fiind în mod automat o persoană împuternicită. Analiza se face de la caz la caz, în funcție de rolul consilierului în proprietate industrială în contextul fiecărei prelucrări de date cu caracter personal, dacă respectiva prelucrare se realizează în calitate de operator sau de persoană împuternicită.

Un rol esențial în calificarea consilierului în proprietate industrială ca fiind operator sau persoană împuternicită îl va avea gradul de control al acestuia în ceea ce privește respectiva prelucrare, și anume:

1) Stabilește consilierul în proprietate industrială care vor fi persoanele vizate de prelucrare? („**CINE?**”)

2) Stabilește consilierul în proprietate industrială ce categorii de date vor fi prelucrate? („**CE?**”)

3) Stabilește consilierul în proprietate industrială pentru ce scop se va realiza prelucrarea? („**PENTRU CE?**”)

4) Stabilește consilierul în proprietate industrială cum se va realiza prelucrarea? („**CUM?**”) – spre exemplu, pentru e perioadă se stochează datele cu caracter personal, etc.

Dacă majoritatea răspunsurilor la întrebările de mai sus sunt DA, atunci consilierul în proprietate industrială acționează ca un operator de date cu caracter personal.

EXEMPLU 1: *Consilierul în proprietate industrială recrutează personal. Acesta va determina ce date îi sunt necesare pentru evaluarea capacității candidatului pentru a ocupa poziția/pozițiile propuse, bineînțeles cu respectarea principiului ca aceste date să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („reducerea la minim a datelor”), scopul prelucrării și cum va realiza prelucrarea. Așadar, consilierul în proprietate industrială va avea calitatea de operator în legătură cu această prelucrare de date cu caracter personal.*

EXEMPLU 2: *Consilierul prelucrează date cu caracter personal ale persoanei recrutate pentru o anumită poziție pentru încheierea contractului individual de muncă conform prevederilor legale aplicabile. Și în acest caz, consilierul în proprietate industrială va avea calitatea de operator în legătură cu această prelucrare de date cu caracter personal.*

EXEMPLU 3: *O societate se adresează unui consilier în proprietate industrială pentru depunerea unei opoziții împotriva înregistrării unei cereri de marcă națională. Consilierul în proprietate industrială este cel care va decide, în principiu, ce date cu caracter personal solicită clientului, care dintre acestea vor fi folosite în cadrul procedurii de opoziție și cum le*

va folosi. Prin urmare, în acest exemplu, consilierul în proprietate industrială va avea calitatea de operator de date cu caracter personal în legătură cu această prelucrare de date.

***EXEMPLU 4**: O societate transmite consilierului în proprietate industrială o solicitare de înregistrare la Oficiul de Stat pentru Invenții și Mărci a unui contract de licență de marcă pentru opozabilitate față de terți. Consilierul în proprietate industrială va redacta și va depune o adresă de înscriere a licenței cu date pe care le ia din contract, cu contractul atașat și cu dovada plății taxei legale de înscriere a licenței. În acest caz, intervenția consilierului în proprietate industrială cu privire la modul de prelucrare al datelor pentru acest scop este minimă. În acest caz, se poate concluziona că consilierul în proprietate industrială va avea calitatea de persoană împuternicită în legătură cu această prelucrare de date.*

III. ASPECTE DE BUNĂ PRACTICĂ SPRE A FI AVUTE ÎN VEDERE PENTRU CONFORMAREA CU PREVEDERILE GDPR

A. PRINCIPII PENTRU PRELUCRAREA DATELOR CU CARACTER PERSONAL

Înainte de a face o prelucrare de date cu caracter personal, consilierul în proprietate industrială trebuie să aibă în vedere principiile ce trebuie să fie respectate în legătură cu orice prelucrare de date cu caracter personal, și anume:

(1) datele cu caracter personal trebuie să fie prelucrate în mod legal, echitabil și transparent față de persoana vizată („legalitate, echitate și transparență”);

(2) să fie colectate în scopuri determinate, explicite și legitime și să nu fie prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale, conform GDPR („limitări legate de scop”);

(3) adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („reducerea la minimum a datelor”);

(4) exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt

inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere („exactitate”);

(5) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu prevederile GDPR, sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor și libertăților persoanei vizate („limitări legate de stocare”);

NOTA!! *GDPR nu stabilește o perioadă standard de stocare a datelor cu caracter personal și nici reguli care să ajute la determinarea acestora. Revine consilierului în proprietate industrială să determine care este perioada de stocare a datelor pe care le prelucrează având în vedere scopul prelucrării acestora, dar și drepturile și libertățile persoanelor vizate. Adoptarea unei politici de stocare, de arhivare a datelor, precum și de ștergere a acestora este recomandabilă.*

(6) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate”).

Consilierul în proprietate industrială are obligația de a face dovada respectării principiilor enunțate mai sus. În acest sens, este recomandabil ca, consilierul în proprietate industrială să realizeze o cartografiere a tuturor fluxurilor de date din cadrul formei sale de organizare și să țină o evidență a operațiunilor de prelucrare a datelor cu caracter personal, chiar dacă nu are această obligație legală conform GDPR.

B. TEMEIURI LEGALE PENTRU PRELUCRAREA DATELOR CU CARACTER PERSONAL DE CĂTRE CONSILIERUL ÎN PROPRIETATE INDUSTRIALĂ DIN ROMÂNIA

Prelucrarea datelor cu caracter personal se poate realiza în mod legal numai dacă se bazează pe unul din temeiurile juridice prevăzute la articolul 6 alin (1) GDPR, și anume:

i. **consimțământul** persoanei vizate pentru unul sau mai multe scopuri specifice;

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

iii. prelucrarea **este necesară** pentru **îndeplinirea unei obligații legale**;

iv. prelucrarea este necesară **pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice**;

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

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

Consilierul în proprietate industrial trebuie să determine de la început care este temeiul juridic în baza căruia se face prelucrarea, ținând cont de scopul urmărit prin prelucrarea datelor cu caracter personal. Fără un temei juridic identificat, prelucrarea este ilegală.

Alegerea temeiului juridic de prelucrare trebuie făcută corect de la început, schimbarea ulterioară a temeiului, fără justificare adecvată, este echivalentă cu o neconformitate.

Alegerea temeiului de prelucrare trebuie documentat (recomandabil prin ținerea evidenței tuturor activităților de prelucrare).

Persoanele vizate trebuie informate cu privire la temeiul prelucrării, ca principiu, înainte de începerea prelucrării.

În cele ce urmează vom analiza câteva dintre temeiurile juridice menționate mai sus.

Așadar:

i. Prelucrarea pe bază de consimțământ

Pentru ca o prelucrare să fie legală în baza unui consimțământ, acesta trebuie să fie liber, specific, informat și lipsit de ambiguitate.

Exprimarea consimțământului unei persoane trebuie să fie exprimată în mod explicit, clar, specific. **Utilizarea unor metode de exprimare implicită/tacită a consimțământului** (spre exemplu căsuțe de acord pre bifate) **nu este o practică legală**.

De asemenea, **furnizarea unui serviciu solicitat de / oferit persoanei vizate nu poate fi condiționată de acordarea consimțământului pentru prelucrarea de date din partea respectivei persoane**, dat fiind că în acest caz consimțământul nu ar mai fi liber exprimat.

Consimțământul **trebuie solicitat în mod specific pentru fiecare scop** pentru care se face prelucrarea.

Dovada obținerii consimțământului trebuie păstrată.

Este de reținut faptul că, conform GDPR **persoana vizată își poate retrage consimțământul în orice moment**, fără a afecta însă legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia. În acest sens, operatorul trebuie să pună la dispoziția persoanei vizate un mecanism de retragere al consimțământului facil și care să dea efect acestei exprimări de voință în cel mai scurt timp.

Având în vedere cele de mai sus, orice prelucrare bazată pe consimțământ ridică numeroase probleme în practică. De aceea, operatorii trebuie să identifice încă de la început dacă consimțământul este într-adevăr temeiul juridic adecvat prelucrării de date cu caracter personal pe care doresc să le realizeze sau dacă ar exista un alt temei juridic mai potrivit.

Determinarea temeiului juridic al prelucrării este importantă dat fiind că această alegere este unică, și, în principiu, nu poate fi schimbată ulterior începerii prelucrării.

EXEMPLU 1: *Consilierul în proprietate industrială stabilește consimțământul ca temei juridic pentru prelucrarea datelor cu caracter personal ale clienților (persoane fizice) pentru prestarea servicii specifice în domeniul proprietății industriale și în acest sens inserează o fereastră de consimțământ expres. Dacă consilierul în proprietate industrială condiționează acordarea serviciilor de existența consimțământului clientului, atunci consimțământul nu este liber exprimat, este viciat. Dacă contractul se execută chiar dacă clientul nu și-a exprimat consimțământul, atunci nu există o libertate reală de alegere a acestuia și prin urmare, consimțământul este viciat.*

În acest caz, temeiul legal al prelucrării este cel al încheierii și executării unui contract, iar nu consimțământul.

! NOTA BENE: *În general, în cadrul relațiilor de muncă, consimțământul ca temei juridic pentru prelucrarea datelor trebuie să fie evitat. Pentru a putea fi considerat a fi valid consimțământul trebuie să fie acordat în mod liber. Ori, dacă persoana vizată nu dispune cu adevărat de libertatea de alegere sau nu este în măsură să refuze sau să își retragă consimțământul fără a fi prejudiciată, acesta nu este considerat a fi acordat în mod liber și prin urmare nu este un consimțământ valid.*

Relația dintre angajat și angajator este văzută în general ca o relație dezechilibrată sub raportul de forțe, dat fiind că angajatorul are mai multă putere decât angajatul. Prin urmare, consimțământul în puține ocazii în cadrul relațiilor de muncă ar putea fi văzut ca o bază legală pentru prelucrarea datelor angajaților.

Ar putea exista însă și situații când prelucrarea datelor angajaților având la bază consimțământul angajatului ar putea fi considerată ca fiind legală, în special dacă este în interesul angajatului. Spre exemplu: în cazul în care consilierul în proprietate industrială oferă un beneficiu angajaților (ex. asigurare facultativă de sănătate, etc).

În cadrul activității unui consilier în proprietate industrială, prelucrările de date având ca temei consimțământul persoanei vizate pot fi diverse, în funcție de modul de organizare și scopurile urmărite.

EXEMPLU 2: *Consilierul în proprietate industrială trimite lunar alerte legislative/jurisprudențiale/promovări din cadrul cabinetului său prin email către clienții săi. În acest sens, va avea nevoie de consimțământul clienților săi pentru trimiterea acestor alerte.*

În legătură cu acest temei juridic de prelucrare, poate fi consultat si Ghidul emis de Grupul de lucru Articolul 29 (WP29) privind consimțământul, dar și cel de transparență, ambele putând fi consultate la adresa - http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360.

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

Justificarea utilizării unui asemenea temei juridic de către consilierul în proprietate industrială pentru o prelucrare de date cu caracter personal constă în **necesitatea** încheierii unui contract solicitat de persoana vizată sau executării unui contract la care persoana vizată este parte.

Prelucrarea de date cu caracter personal nu se poate baza pe acest temei juridic dacă privește datele unei alte persoane decât cea care încheie contractul.

***EXEMPLU 1**: Prelucrarea datelor reprezentantului clientului care semnează contractul de prestări servicii în domeniul proprietății industriale pentru client se face pentru executarea contractului.*

iii. <u>Prelucrarea este necesară pentru îndeplinirea unei obligații legale</u>

Prelucrarea datelor cu caracter personal în temeiul acestui temei juridic de către consilierul în proprietate industrială se poate realiza dacă există o obligație legală în legătură cu care acesta trebuie să se conformeze, inclusiv o decizie administrativă sau judecătorească în acest sens.

***EXEMPLU 1:** Consilierul în proprietate industrială poate să acționeze în baza unei procuri care trebuie să conțină anumite elemente conform normelor în vigoare, printre care și date cu caracter personal ale clientului. Așadar, datele prelucrate de către consilier în legătură cu procura de reprezentare se face pentru îndeplinirea unei obligații legale.*

***EXEMPLU 2**: Consilierul în proprietate industrială este obligat conform normelor legale în vigoare să țină evidența zilnică a timpului de muncă al salariaților săi, cu precizarea orei de începere a activității și a celei de finalizare. Așadar, prelucrarea datelor cu caracter personal ale salariaților săi în scop de pontaj se face pentru îndeplinirea unei obligații legale.*

iv. <u>Prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță</u>

Interesul legitim este cel mai flexibil temei juridic de prelucrare a datelor cu caracter personal și de aceea trebuie folosit în mod adecvat de către consilierul în proprietate industrială, evaluând de fiecare dată care este impactul folosirii acestui temei juridic asupra drepturilor și libertăților persoanelor vizate. Acesta poate fi folosit când impactul asupra persoanelor vizate este minim.

***EXEMPLU 1:** Consilierul în proprietate industrială are în cadrul formei sale de organizare o bibliotecă cu numeroase materiale. Consilierul va prelucra în condiții de securitate numele, prenumele salariaților săi care împrumuta materiale, precum și data împrumutului și data returnării materialului în temeiul interesului său legitim de a ține o evidență a materialelor sale și pentru a-și proteja proprietatea.*

C. INFORMAREA PERSOANELOR VIZATE

1) PRECIZĂRI GENERALE

Indiferent de temeiul juridic al prelucrării de date cu caracter personal, operatorii trebuie să se conformeze unei obligații specifice de informare a persoanelor vizate în legătură cu prelucrările efectuate.

Informarea trebuie să fie oferită într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu.

Informațiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic. La solicitarea persoanei vizate, informațiile pot fi furnizate verbal, cu condiția ca identitatea persoanei vizate să fie dovedită prin alte mijloace.

2) CUM ÎȘI POATE ÎNDEPLINI OBLIGAȚIA DE INFORMARE CONSILIERUL?

Consilierul în proprietate industrială își poate îndeplini această obligație spre exemplu prin (i) introducerea / anexarea notei de informare la contractul de prestări servicii, (ii) includerea unei politici de confidențialitate / politici privind protecția datelor cu caracter personal pe website-ul formei sale de organizare, (iii) introducerea notei de informare în regulamentul intern pentru salariați care sa fie adus la cunoștința salariaților.

3) CE CONȚINUT TREBUIE SĂ AIBĂ INFORMAREA?

În funcție de sursa obținerii datelor, și anume de la persoana vizată sau din alte surse, informarea trebuie să aibă un conținut specific conform articolelor 13 și 14 din GDPR.

TIP DE INFORMAȚIE	DATE OBȚINUTE DE LA PERSOANA VIZATĂ	DATE OBȚINUTE DIN ALTE SURSE
identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia	√	√
datele de contact ale responsabilului cu protecția datelor, după caz	√	√
scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării	√	√

în cazul în care prelucrarea se face în temeiul interesele legitime urmărite de operator sau de o parte terță, precizarea intereselor legitime urmărite	√	√
categoriile de date cu caracter personal vizate		√
destinatarii sau categoriile de destinatari ai datelor cu caracter personal	√	√
Informații specific privind transferurile de date cu caracter personal către o țară terță sau o organizație internațională, dacă este cazul	√	√
perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă	√	√
existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării sau a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor	√	√
atunci când prelucrarea are		

ca temei juridic consimțământul, existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia	√	√
dreptul de a depune o plângere în fața unei autorități de supraveghere	√	√
sursa din care provin datele cu caracter personal și, dacă este cazul, dacă acestea provin din surse disponibile public		√
dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații	√	
existența unui proces decizional automatizat incluzând crearea de profiluri, 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	√	√

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

Un draft de notă de informare ce trebuie să fie adaptat de fiecare consilier în proprietate industrială conform formei sale de organizare și activităților sale de prelucrare a datelor cu caracter personal, poate fi găsit în cadrul Anexei 1 la acest Ghid.

4) CÂND SE FACE INFORMAREA?

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

În cazul în care datele cu caracter personal sunt colectate din alte surse, informarea se face:

a. 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;

b. 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

c. dacă se intenționează divulgarea datelor cu caracter personal către un alt destinatar, cel mai târzi divulgate pentru prima oară.

5) EXCEPȚII DE LA OBLIGAȚIA DE INFORMARE

Dacă persoana vizată deține deja informațiile, obligația de informare nu mai este aplicabilă.

În cazul datelor cu caracter personal obținute din alte surse, obligația de informare nu este aplicabilă:

a. dacă furnizarea acestor informații se dovedește a fi imposibilă sau ar implica eforturi disproportionate sau în măsura în care obligația de informare este susceptibil 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, inclusiv punerea informațiilor la dispoziția publicului;

b. obținerea sau divulgarea datelor este prevăzută în mod expres de dreptul Uniunii sau de dreptul intern sub incidența căruia intră operatorul și care prevede măsuri adecvate pentru a proteja interesele legitime ale persoanei vizate; sau

c. în cazul în care datele cu caracter personal trebuie să rămână confidențiale în temeiul unei obligații statutare de secret profesional reglementate de dreptul Uniunii sau de dreptul intern, inclusiv al unei obligații legale de a păstra secretul.

D. DREPTURILE PERSOANELOR VIZATE

1) CARE SUNT DREPTURILE PERSOANELOR VIZATE CONFORM GDPR?

GDPR conferă următoarele drepturi persoanelor vizate:

1) **dreptul de acces** – care permite persoanei vizate să obțină din partea operatorului o confirmare a faptului că datele sale cu caracter personal sunt prelucrate sau nu și, în caz afirmativ, informații relevante (prevăzute la art. 15 GDPR) privind activitățile de prelucrare a datelor, precum și o copie a datelor cu caracter personal ce fac obiectul prelucrării, fără însă a aduce atingere drepturilor și libertăților altora.

   NOTA BENE!!! *Consilierul în proprietate industrială trebuie să aibă în vedere faptul că, conform articolului 17 din Ordonanta 66/2000 privind organizarea și exercitarea profesiei de consilier în proprietate industrială, astfel cum este în prezent în vigoare, este obligat să nu divulge datele și informațiile primite de la clientul său sau referitoare la acesta decât în limitele mandatului și în condițiile prevăzute de lege. Prin urmare, consilierul în proprietate industrială trebuie să aibă în vedere acest aspect atunci când răspunde la o solicitare de acces la date.*

2) **dreptul la rectificare** – care permite persoanei vizate să obțină de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc sau completarea datelor sale care sunt incomplete;

3) **dreptul la ștergerea datelor (dreptul de a fi uitat)** – care permite persoanei vizate să obțină din partea operatorului 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 anumite cazuri (de exemplu, dacă datele nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate);

4) **dreptul la restricționarea prelucrării** - care permite persoanei vizate să obțină din partea operatorului restricționarea prelucrării datelor cu caracter personal în anumite cazuri (de exemplu, în situația în care persoana vizată contestă exactitatea datelor cu caracter personal, pentru o perioadă care îi permite operatorului să verifice corectitudinea datelor);

5) **dreptul la opoziție** - care permite persoanei vizate sa se opună la prelucrarea datelor cu caracter personal în condițiile și limitele prevăzute de lege;

6) **dreptul la portabilitatea datelor** – care permit persoanei vizate să primească datele personale pe care le-a furnizat într-un format structurat, utilizat în mod curent și care poate fi citit de calculator sau de a transmite aceste date unui alt operator de date personale;

7) **dreptul de a depune o plângere în fața unei autorități competente**;

8) **dreptul de a-și retrage consimțământul în orice moment**, dacă prelucrarea de date are acest temei juridic, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;

9) **dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrare automată**, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă.

2) ÎN CÂT TIMP TREBUIE SĂ RĂSPUNDĂ CONSILIERUL ÎN PROPRIETATE INDUSTRIALĂ OPERATOR LA O CERERE A UNEI PERSOANE VIZATE PRIN CARE ÎȘI EXERCITĂ DREPTURILE?

Conform articolului 12 GDPR, operatorul trebuie să îi furnizeze persoanei vizate informațiile conform cererii depuse în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu două luni atunci când este necesar, ținându-se seama de complexitatea și numărul cererilor. Operatorul informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând și motivele întârzierii. În cazul în care persoana vizată introduce o cerere în format electronic, informațiile sunt furnizate în format electronic acolo unde este posibil, cu excepția cazului în care persoana vizată solicită un alt format.

Dacă operatorul nu ia măsuri cu privire la cererea persoanei vizate, operatorul informează persoana vizată, fără întârziere și în termen de cel mult o lună de la primirea cererii, cu privire la motivele pentru care nu ia măsuri și la posibilitatea de a depune o plângere în fața unei autorități de supraveghere și de a introduce o cale de atac judiciară.

3) RECOMANDĂRI CU PRIVIRE LA RĂSPUNSURILE PRIVIND CERERILE DE EXECRITARE A DREPTURILOR PERSOANELOR VIZATE

Consilierul în proprietate industrială trebuie să implementeze un mecanism ușor de exercitare a drepturilor de către persoana vizată. Spre exemplu, comunicarea unei adrese de email, poștale, indicarea unei persoane pentru exercitarea drepturilor.

De asemenea, este recomandabil să fie implementată o politică internă cu privire la modul în care consilierul în proprietate industrială răspunde cererilor de exercitare a drepturilor de către persoanele vizate, inclusiv cine, cum și în ce termen.

Este recomandabil ca consilierul în proprietate industrială să păstreze o evidență a gestionării cererilor de exercitare a drepturilor persoanelor vizate și să aibă dovezi care să ateste îndeplinirea obligațiilor sale.

E. EVIDENȚELE ACTIVITĂȚILOR DE PRELUCRARE A DATELOR CU CARACTER PERSONAL

Deși conform articolului 30, alin 5 GDPR obligația de ținere a unei evidențe a activităților de prelucrare a datelor cu caracter personal se aplică doar unei întreprinderi sau organizații cu mai mult de 250 de angajați sau în cazul în care prelucrarea este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, nu este ocazională sau prelucrarea include categorii speciale de date sau date cu caracter personal referitoare la condamnări penale și infracțiuni, este recomandabil ca fiecare consilier în proprietate industrial să țină o astfel de evidență a activităților de prelucrare a datelor cu caracter personal în scris, inclusiv în format electronic.

1) INFORMAȚIILE CARE TREBUIE SĂ SE REGĂSEASCĂ ÎN EVIDENȚA ACTIVITĂȚILOR DE PRELUCRARE ALE UNUI OPERATOR

Evidența operațiunilor de prelucrare realizate de către un operator trebuie să cuprindă cel puțin următoarele informații:

- numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;

- scopurile prelucrării;

- o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;

- categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale;

- dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, acolo unde este cazul, documentația care dovedește existența unor garanții adecvate;

- acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;

- acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate luate de operator;

- numele și datele de contact ale persoanei sau persoanelor împuternicite de operator și ale persoanei împuternicite de operator, după caz.

2) INFORMAȚIILE CARE TREBUIE SĂ SE REGĂSEASCĂ ÎN EVIDENȚA ACTIVITĂȚILOR DE PRELUCRARE ALE UNEI PERSOANE ÎMPUTERNICITE

Evidența operațiunilor de prelucrare realizate de către o persoană împuternicită trebuie să cuprindă cel puțin următoarele informații:

- numele și datele de contact ale fiecărui operator în numele căruia acționează această persoană (aceste persoane), precum și ale reprezentantului operatorului, după caz;

- categoriile de activități de prelucrare desfășurate în numele fiecărui operator;

- 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, acolo unde este cazul, documentația care dovedește existența unor garanții adecvate;

- acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate luate de operator.

F. SECURITATEA DATELOR CU CARACTER PERSONAL

1) ASPECTE GENERALE

Consilierul în proprietate industrială, fie că are calitatea de operator sau de persoană împuternicită, trebuie să implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător, ținând cont de 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, 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.

La evaluarea nivelului adecvat de securitate, se ține seama în special de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

Aderarea la un cod de conduită aprobat sau la un mecanism de certificare aprobat, poate fi utilizată ca element prin care să se demonstreze îndeplinirea cerințelor prevăzute de securitate prevăzute de GDPR.

Consilierul în proprietate industrial, fie că are calitatea de operator, fie de persoană împuternicită trebuie să ia măsuri pentru a asigura că orice persoană fizică care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator și care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care această obligație îi revine în temeiul dreptului Uniunii sau al dreptului intern.

Consilierul în proprietate industrială trebuie să aibă în vedere faptul că, conform articolului 17 din Ordonanța 66/2000 privind organizarea și exercitarea profesiei de consilier în proprietate industrială, astfel cum este în prezent în vigoare, este obligat să nu

divulge datele și informațiile primite de la clientul său sau referitoare la acesta decât în limitele mandatului și în condițiile prevăzute de lege. Prin urmare, consilierul în proprietate industrială este supus obligației de confidențialitate și trebuie să se asigure că și-o îndepliniște prin implementarea de măsuri în acest sens.

2) RECOMANDĂRI

Consilierul în proprietate trebuie să implementeze măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător datelor cu caracter personal pe care le prelucrează.

Redăm mai jos câteva recomandări de măsuri organizatorice și de securitate ce ar putea fi avute în vedere de consilierul în proprietate industrial, bineînțeles depinzând de activitatea de prelucrare pe care o face:

- să limiteze accesul în cadrul cabinetului / societății sale;

- să nu stocheze sau să arhiveze documente / dosare ce conțin date cu caracter personal în spații accesibile tuturor;

- să promoveze politica biroului curat (clean desk);

- să instaleze sisteme de alarmă în cadrul locației unde își desfășoară activitatea;

- să acorde acces la date doar persoanelor din cadrul cabinetului / societății sale care chiar au nevoie să aibă acces și să fie implementate măsuri organizatorice în acest sens cu privire la rolul fiecăreia. Persoanele cu drept de acces la date trebuie să fie instructate cu privire la normele privind protecția datelor cu caracter personal, iar aceste instructaje trebuie reluate la anumite intervale;

- să securizeze stațiile de lucru prin parole de acces care să fie cunoscute doar de persoana cu drept de acces la acea stație de lucru, parolă care să aibă cel puțin opt caractere care să conțină cel puțin o literă mare, una mica, o cifră, un caracter special; parolele să nu fie notate pe foi; să nu fie înregistrate și mai apoi accesul să se facă automat fără introducerea parolei; să fie schimbate în mod regulat;

- să fie securizat orice unitate externă de stocare a datelor (spre exemplu hard disk extern, stick USB, CD-uri, DVD-uri, etc);

- determinarea locației exacte a serverelor și a măsurilor de securitate cu privire la acestea;

- implementarea unei politici de securitate;

- acoperirea aspectelor de securitate a datelor în contractele încheiate cu furnizorii de servicii de IT.

G. ÎNCĂLCAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL

În cazul în care are loc **o încălcare a securității datelor cu caracter personal**, 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**, operatorul notifică acest lucru autorității de supraveghere competente, fără întârzieri nejustificate și, dacă este posibil, **în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta**, **cu excepția cazului în care este puțin probabil să genereze un risc pentru drepturile și libertățile persoanelor fizice**. În cazul în care notificarea nu are loc în termen de 72 de ore, aceasta este însoțită de o explicație motivată din partea autorității de supraveghere în cazul în care.

Persoana împuternicită trebuie să înștiințeze operatorul fără întârzieri nejustificate după ce ia cunoștință de o încălcare a securității datelor cu caracter personal.

Încălcările de securitate pot avea cauze diverse de la nefuncționarea sau funcționarea necorespunzătoare a sistemelor informatice până la erori umane, spre exemplu: pierderea unor documente, transmiterea unei corespondențe la adresa greșită, accesul la dosare ce cuprind date cu caracter personal de către persoane ce nu au drept de acces, atacuri informatice, pierderea unui stick USB cu date cu caracter personal care nu avea implementate măsuri de securitate ce ar fi făcut datele neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea, etc.

ANSPDCP a pus la dispoziție un formular prin care să fie notificate aceste încălcări de securitate a datelor care poate fi accesat la acest link - http://www.dataprotection.ro/servlet/ViewDocument?id=1516.

De asemenea, poate fi consultat si Ghidul emis de Grupul de lucru Articolul 29 (WP29) privind notificarea încălcărilor de securitate ce poate fi consultat în versiunea în limba română de pe website-ul ANSPDCP - http://www.dataprotection.ro/?page=Ghiduri_ale_grupului_de_lucru_art_29_februarie_2018&lang=ro, dar și versiunea în limba engleză la această adresă – http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360.

Operatorul trebuie să **documenteze** toate cazurile de încălcare a securității datelor cu caracter personal. Aceste documentări trebuie să cuprindă o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse.

În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze **un risc ridicat** pentru drepturile și libertățile persoanelor fizice, operatorul trebuie **să informeze persoana vizată** fără întârzieri nejustificate cu privire la această încălcare.

Informarea persoanei vizate nu este necesară în cazul în care oricare dintre următoarele condiții este îndeplinită:

a. operatorul a implementat măsuri de protecție tehnice și organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin **neinteligibile** oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;

b. operatorul a luat **măsuri ulterioare** prin care se asigură că **riscul ridicat** pentru drepturile și libertățile persoanelor vizate **nu mai este susceptibil să se materializeze**;

c. **ar necesita un efort disproporționat**. În această situație, se efectuează în loc o **informare publică** sau se ia o **măsură similară** prin care persoanele vizate sunt informate într-un mod la fel de eficace.

Este foarte important ca operatorul să identifice imediat orice încălcare a securității datelor cu caracter personal și să ia imediat toate măsurile care se impun.

În acest sens, operatorul trebuie să instructeze persoanele implicate în activitatea de prelucrare a datelor cu caracter personal astfel încât acestea să poată identifica orice încălcare a securității datelor cu caracter personal și să le aducă la cunoștință toate măsurile necesare în vederea analizei și limitării consecințelor încălcării securității datelor cu caracter personal și eventual notificarea autorității de supraveghere și a persoanelor vizate, dacă este cazul.

H. EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR CU CARACTER PERSONAL

În funcție de 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.

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

Evaluarea impactului asupra protecției datelor menționată **se impune mai ales în cazul**:

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

b. **prelucrării pe scară largă a unor categorii speciale de date astfel cum sunt menționate în GDPR sau a unor date cu caracter personal privind condamnări penale și infracțiuni**; sau

c. **unei monitorizări sistematice pe scară largă a unei zone accesibile publicului**.

Evaluarea conține cel puțin:

a. **o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator**;

b. **o evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri**;

c. **o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate**; și

d. **măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentului regulament, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor persoane interesate**.

Operatorul consultă autoritatea de supraveghere înainte de prelucrarea atunci când evaluarea impactului asupra protecției datelor indică faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri luate de operator pentru atenuarea riscului.

Autoritatea de supraveghere oferă consultanță prealabilă atunci când consideră că prelucrarea ar încălca GDPR, în special atunci când riscul nu a fost identificat sau atenuat într-o măsură suficientă de către operator.

Conform articolului 35 GDPR, autoritatea de supraveghere întocmește și publică o listă a tipurilor de operațiuni de prelucrare care fac obiectul cerinței de efectuare a unei evaluări a impactului asupra protecției datelor. Până la momentul redactării prezentului ghid, ANSPDCP nu a publicat o asemenea listă. Asemenea liste au fost publicate de autorități din alte state membre UE, cum ar fi, Marea Britanie, Franța, Polonia, Austria, Belgia, Irlanda, Germania, etc.

Grupul de lucru Articolul 29 (WP29) a emis de asemenea un Ghid privind evaluarea impactului asupra protecției datelor ce poate fi accesat la următorul link - http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360.

I. RESPONSABILUL CU PROTECȚIA DATELOR CU CARACTER PERSONAL

1) ASPECTE GENERALE

Numirea unui responsabil cu protecția datelor cu caracter personal reprezintă o obligație numai în anumite situații prevăzute de GDPR. Cu toate acestea, numirea voluntară a unui responsabil cu protecția datelor cu caracter personal este o recomandare de bună practică.

Operatorul și persoana împuternicită de operator au obligația desemnării unui responsabil cu protecția datelor ori în următoarele situații:

1) **prelucrarea este efectuată de o autoritate sau un organism public**, cu excepția instanțelor care acționează în exercițiul funcției lor jurisdicționale;

2) **activitățile principale** ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrare care, prin **natura, domeniul de aplicare și/sau scopurile lor,** necesită o **monitorizare periodică și sistematică a persoanelor vizate pe scară largă;** sau

3) activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în **prelucrarea pe scară largă a unor categorii speciale de date**, menționate la articolul 9 GDPR, sau a **unor date cu caracter personal privind condamnări penale și infracțiuni**, menționate la articolul 10 GDPR.

Fiecare consilier în proprietate industrială trebuie să evalueze fiecare în parte, necesitatea sau oportunitatea numirii unui responsabil cu protecția datelor cu caracter personal prin raportare la dimensiunea sa, modul său de organizare, tipul de prelucrări de date cu

caracter personal, volumul și varietatea acestora, durata prelucrării și stocării acestora, aria geografică acoperită.

Formele individuale de exercitare a profesiei, spre exemplu cabinetul individual, în principiu, nu are obligația numirii unui responsabil cu protecția datelor cu caracter personal.

Formele mai complexe de exercitare a profesiei (formate dintr-un număr semnificativ de consilieri, departamente auxiliare – IT, contabilitate, marketing, etc) sunt susceptibile în a intra sub incidența obligației de a numi un responsabil cu protecția datelor.

Grupul de lucru Articolul 29 (WP29) a emis de asemenea un Ghid privind responsabilul cu protecția datelor cu caracter personal, ce explicitează o serie de noțiuni cum ar fi, cea de activitate principală, prelucrare pe scară largă, monitorizare periodică și sistematică, etc, ghid ce poate fi consultat accesând următorul link - http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360.

Dacă se ia decizia numirii unui responsabil cu protecția datelor trebuie să se aibă în vedere că acesta este desemnat **pe baza calităților profesionale** și, în special, a **cunoștințelor de specialitate în dreptul și practicile din domeniul protecției datelor**, precum și pe baza capacității de a îndeplini sarcinile prevăzute de GDPR.

Responsabilul cu protecția datelor poate fi un **membru al personalului** operatorului sau persoanei împuternicite de operator sau **poate să își îndeplinească sarcinile în baza unui contract de servicii.**

Odată numit, operatorul sau persoana împuternicită de operator publică datele de contact ale responsabilului cu protecția datelor, spre exemplu pe website, în comunicările interne, externe, etc și le comunică și autorității de supraveghere.

2) FUNCȚIA RESPONSABILULUI CU PROTECȚIA DATELOR

Operatorul și persoana împuternicită de operator trebuie să se asigură că responsabilul cu protecția datelor **este implicat în mod corespunzător** și **în timp util** în toate aspectele legate de protecția datelor cu caracter personal.

Operatorul și persoana împuternicită de operator trebuie să **sprijine** responsabilul cu protecția datelor în îndeplinirea sarcinilor sale, asigurându-i **resursele necesare** pentru executarea acestor sarcini, precum și **accesarea datelor cu caracter personal** și a **operațiunilor de prelucrare**, și pentru **menținerea cunoștințelor sale de specialitate**.

Operatorul și persoana împuternicită de operator trebuie să se asigure că responsabilul cu protecția datelor **nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea acestor sarcini**.

Acesta **nu poate fi demis sau sancționat** de către operator sau de persoana împuternicită de operator pentru îndeplinirea sarcinilor sale.

Responsabilul cu protecția datelor **răspunde direct în fața celui mai înalt nivel al conducerii** operatorului sau persoanei împuternicite de operator.

Persoanele vizate **pot contacta** responsabilul cu protecția datelor cu privire la toate chestiunile legate de prelucrarea datelor lor și la exercitarea drepturilor lor în temeiul prezentului regulament.

Responsabilul cu protecția datelor are **obligația de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale**, în conformitate cu dreptul Uniunii sau cu dreptul intern.

Responsabilul cu protecția datelor poate îndeplini și alte sarcini și atribuții. Operatorul sau persoana împuternicită de operator trebuie însă să se asigure că niciuna dintre aceste sarcini și atribuții **nu generează un conflict de interese**.

3) SARCINILE RESPONSABILULUI CU PROTECȚIA DATELOR

Responsabilul cu protecția datelor are cel puțin următoarele sarcini:

a. **informarea și consilierea** operatorului, sau a persoanei împuternicite de operator, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul prezentului regulament și al altor dispoziții de drept al Uniunii sau drept intern referitoare la protecția datelor;

b. **monitorizarea respectării GDPR**, a altor dispoziții de drept al Uniunii sau de drept intern referitoare la protecția datelor și a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce privește protecția datelor cu caracter personal, inclusiv **alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente**;

c. **furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia**;

d. **<u>cooperarea cu autoritatea de supraveghere</u>**;

e. **<u>asumarea rolului de punct de contact</u>** pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menționată în cazul evaluării de impact, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.

La preluarea funcției de responsabil cu protecția datelor cu caracter personal acesta trebuie să:

i. auditeze organizația, să identifice situația existentă cu privire la fluxurile de date, inclusiv vulnerabilitățile de conformare identificate și să facă recomandări pentru conformare, inclusiv de minimizare a datelor colectate. În acest sens, responsabilul cu protecția datelor trebuie să organizeze interviuri cu personalul din departamentele relevante ale organizației pentru a colecta informații, dar și să analizeze documente relevante care să permită auditul;

ii. consilieze conducerea operatorului/persoanei împuternicite (cel care l-a numit) cu privire la obligațiile specifice și la vulnerabilitățile identificate precum și cu privire la planul de conformare și să prioritizeze acțiunile de conformare.

Urmare a recomandărilor făcute, responsabilul cu protecția datelor trebuie să coordoneze procesul de implementare, inclusiv evidența activităților de prelucrare, să redacteze documentația specifică (politici interne, note de informare, consimțăminte, revizuire contracte furnizori, etc), să acorde asistență cu privire la evaluarea de impact, acolo unde este necesară, asistență în cazului unui incident de securitate, etc.

J. TRANSFERUL DE DATE CU CARACTER PERSONAL CĂTRE ȚĂRI TERȚE

1) TRANSFERUL DE DATE ÎN TEMEIUL UNEI DECIZII PRIVIND NIVELUL ADECVAT AL NIVELULUI DE PROTECȚIE

Orice date cu caracter personal care fac obiectul prelucrării sau care urmează a fi prelucrate pot fi transferate către o țară terță (în afara Uniunii Europene, Norvegiei, Liechtenstein-ului și Islandei între care orice transfer de date este considerat a fi un transfer de date in interiorul UE) sau o organizație internațională în legătură cu care Comisia Europeană a decis că țara terță, un teritoriu ori unul sau mai multe sectoare specificate din acea țară terță sau organizația internațională în cauză asigură un nivel de protecție adecvat fără nicio autorizare specială.

Până în prezent, Comisia Europeană a recunoscut un nivel adecvat de protecție următoarelor țări: Andorra, Argentina, Canada (organizații comerciale), Insulele Faroe, Guernsey, Israel, Insula Man, Jersey, Noua Zeelandă, Elveția, Uruguay și SUA (aceasta din

urmă limitată la cadrul oferit de Privacy Shield). Discuții cu privire la recunoaștere unui nivel adecvat de protecție se poartă în prezent cu Japonia și Koreea de Sud.

2) **TRANSFERUL ÎN BAZA UNEI GARANȚII ADECVATE**

În absența unei decizii prin care Comisia Europeană a decis că țara terță, un teritoriu ori unul sau mai multe sectoare specificate din acea țară terță sau organizația internațională în cauză asigură un nivel de protecție adecvat, operatorul sau persoana împuternicită de operator poate transfera date cu caracter personal către o țară terță sau o organizație internațională numai dacă operatorul sau persoana împuternicită de operator a oferit **garanții adecvate și cu condiția să existe drepturi opozabile și căi de atac eficiente pentru persoanele vizate**.

Garanțiile adecvate pot fi furnizate fără să fie nevoie de nicio autorizație specifică din partea unei autorități de supraveghere, prin:

a. un instrument obligatoriu din punct de vedere juridic și executoriu între autoritățile sau organismele publice;

b. reguli corporatiste obligatorii;

c. clauze standard de protecție a datelor adoptate de Comisia Europeană;

d. clauze standard de protecție a datelor adoptate de o autoritate de supraveghere și aprobate de Comisia Europeană;

e. un cod de conduită aprobat, însoțit de un angajament obligatoriu și executoriu din partea operatorului sau a persoanei împuternicite de operator din țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate; sau

f. un mecanism de certificare aprobat, însoțit de un angajament obligatoriu și executoriu din partea operatorului sau a persoanei împuternicite de operator din țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate.

Sub rezerva autorizării din partea autorității de supraveghere competente, garanțiile adecvate pot fi furnizate de asemenea, în special, prin:

a. clauze contractuale între operator sau persoana împuternicită de operator și operatorul, persoana împuternicită de operator sau destinatarul datelor cu caracter personal din țara terță sau organizația internațională; sau

b. dispoziții care urmează să fie incluse în acordurile administrative dintre

autoritățile sau organismele publice, care includ drepturi opozabile și efective pentru persoanele vizate.

3) **DEROGĂRI SITUAȚII SPECIFICE**

În absența unei decizii privind caracterul adecvat al nivelului de protecție sau a unor garanții adecvate inclusiv a regulilor corporatiste obligatorii, un transfer sau un set de transferuri de date cu caracter personal către o țară terță sau o organizație internațională poate avea loc numai în una dintre condițiile următoare:

a. persoana vizată și-a exprimat **în mod explicit acordul cu privire la transferul propus**, după ce a fost informată asupra posibilelor riscuri pe care astfel de transferuri le pot implica pentru persoana vizată ca urmare a lipsei unei decizii privind caracterul adecvat al nivelului de protecție și a unor garanții adecvate;

b. transferul este **necesar pentru executarea unui contract** între persoana vizată și operator sau **pentru aplicarea unor măsuri precontractuale** adoptate la cererea persoanei vizate;

c. transferul este necesar pentru **încheierea unui contract sau pentru executarea unui contract** încheiat în interesul persoanei vizate între operator și o altă persoană fizică sau juridică;

d. transferul este necesar din considerente importante de **interes public**;

e. transferul este necesar pentru **stabilirea, exercitarea sau apărarea unui drept în instanță**;

f. transferul este necesar pentru **protejarea intereselor vitale** ale persoanei vizate sau ale altor persoane, atunci când persoana vizată **nu are capacitatea fizică sau juridică de a-și exprima acordul**;

g. transferul se realizează **dintr-un registru** care, potrivit dreptului Uniunii sau al dreptului intern, are scopul de a furniza informații publicului și care poate fi consultat fie de public în general, fie de orice persoană care poate face dovada unui interes legitim, dar numai în măsura în care sunt îndeplinite condițiile cu privire la consultare prevăzute de dreptul Uniunii sau de dreptul intern în acel caz specific.

În cazul în care un transfer nu ar putea să se întemeieze pe o decizie privind caracterul adecvat al nivelului de protecție sau a unor garanții adecvate inclusiv a regulilor corporatiste obligatorii, și nu este aplicabilă niciuna dintre derogările pentru situații

specifice prevăzute mai sus, un transfer către o țară terță sau o organizație internațională poate avea loc numai în cazul în care:

- **transferul nu este repetitiv**,
- se referă doar la un **număr limitat de persoane vizate**,
- este necesar în scopul **realizării intereselor legitime majore** urmărite de operator asupra căruia nu prevalează interesele sau drepturile și libertățile persoanei vizate și operatorul a evaluat toate circumstanțele aferente transferului de date și, pe baza acestei evaluări, a prezentat **garanții corespunzătoare** în ceea ce privește protecția datelor cu caracter personal. Operatorul informează autoritatea de supraveghere cu privire la transfer. Operatorul, în plus față de furnizarea informațiilor menționate la articolele 13 și 14 din GDPR, informează persoana vizată cu privire la transfer și la interesele legitime majore pe care le urmărește.