

Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova

**GHID PRIVIND EVALUAREA IMPACTULUI
ASUPRA PROTECȚIEI DATELOR CU CARACTER PERSONAL (DPIA)**



Prezentul Ghid a fost elaborat cu susținerea Proiectului UE TWINNING MD 13ENPI JH0317 (MD29) "Consolidarea Capacităților Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova"

I. Conținut	4
A. Introducere	4
B. Uniunea Europeană: GDPR	5
C. Republica Moldova: Legea privind protecția datelor cu caracter personal	6
II. Atribuțiile CNPDCP	7
A. Lista tipurilor de operațiuni de prelucrare	7
1. Abordarea europeană	7
2. Abordarea UK	9
3. Abordarea Germană	9
B. Consultarea Prealabilă	10
III. Atribuțiile Operatorului	11
A. Necesitatea efectuării unei DPIA: risc ridicat pentru drepturile și libertățile persoanelor fizice	11
B. Realizarea unei DPIA	12
1. Descrierea sistematică a operațiunilor de prelucrare prevăzute și scopul prelucrării, inclusiv, dacă este cazul, interesul legitim urmărit de operator	14
2. Evaluarea necesității și proporționalității operațiunilor de prelucrare în raport cu scopurile.....	14
3. Evaluarea riscurilor la adresa drepturilor și libertăților subiecților de date.....	15
4. Măsurile prevăzute pentru abordarea riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele pentru asigurarea protecției datelor cu caracter personal și pentru a demonstra conformitatea cu legea ținând cont de drepturile și interesele legitime ale subiecților de date	16
5. Implicarea părților interesate	20

I. Conținut

A. Introducere

Evaluarea impactului asupra protecției datelor este un proces destinat să descrie operațiunile de prelucrare preconizate, să evalueze necesitatea și proporționalitatea acestora și să contribuie la gestionarea riscurilor privind drepturile și libertățile subiecților de date rezultate din prelucrarea datelor cu caracter personal, prin evaluarea acestora și stabilirea de măsuri pentru atenuarea lor.

Evaluarea impactului asupra protecției datelor reprezintă un instrument important pentru responsabilizare, deoarece ajută operatorii de date cu caracter personal nu numai să respecte cerințele Legii nr. 133/2011 privind protecția datelor cu caracter personal (în continuare – Legea nr. 133/2011), ci și să demonstreze că au fost luate măsuri adecvate pentru a asigura conformitatea cu prevederile legale naționale, precum și cu cele europene - Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor – în continuare GDPR) .

Cu alte cuvinte, evaluarea impactului asupra protecției datelor reprezintă un proces pentru consolidarea/construirea și demonstrarea conformității. O evaluare a impactului asupra protecției datelor ar trebui, în mod ideal, să fie efectuată în faza de proiectare a unui nou sistem de evidență/bază de date ce implică prelucrarea datelor cu caracter personal și, ulterior, revizuită atunci când cerințele privind sistemul de evidență/baza de date și/sau obligațiile legale suferă modificări.

Pentru a asigura respectarea Legii nr. 133/2011, în cazul în care prelucrarea este susceptibilă să genereze un risc sporit pentru drepturile și libertățile persoanelor fizice, operatorul este responsabil de realizarea unei evaluări a impactului asupra protecției datelor pentru a determina/estima, în special, originea, natura, specificitatea/particularitatea și gravitatea acestui risc.

Este deosebit de relevantă realizarea unei evaluări a impactului asupra protecției datelor atunci când se introduce o nouă tehnologie de prelucrare a datelor cu caracter personal și în cazul în care evaluarea impactului asupra protecției datelor nu a fost efectuată anterior de către operator sau în cazul în care aceasta devine necesară ținând cont de timpul care s-a scurs de la prelucrarea inițială. În astfel de cazuri, operatorul trebuie să efectueze o evaluare a impactului asupra protecției datelor anterior prelucrării, pentru a evalua/aprecia probabilitatea și gravitatea riscului, luând în considerație natura, scopul, contextul, obiectivele prelucrării și sursele de risc. Această evaluare a impactului asupra protecției datelor ar trebui să includă, în special, măsurile, garanțiile și mecanismele prevăzute pentru diminuarea acestui risc, în vederea asigurării protecției datelor cu caracter personal și a demonstrării conformității prelucrării datelor cu caracter personal cu legislația în vigoare.

În cazul în care o evaluare a impactului asupra protecției datelor indică faptul că operațiunile de prelucrare a datelor cu caracter personal implică un risc sporit pe care operatorul nu îl poate reduce prin măsuri adecvate, luând în considerație tehnologia disponibilă și costurile de punere în aplicare, este necesară o consultare prealabilă a Centrului Național pentru Protecția Datelor cu Caracter Personal (în continuare – CNPDCP) anterior prelucrării.

Având în vedere că obligația efectuării unei evaluări a impactului asupra protecției datelor a fost preluată în legislația națională din reglementările Uniunii Europene (UE), și anume, din Regulamentul general privind protecția datelor, se menționează că, procesul de armonizare a legislației naționale în domeniul protecției datelor cu caracter personal cu acquis-ul european nu este finalizat, astfel, pentru o înțelegere mai bună de către operatori/persoane împuternicite de operatori a obligației efectuării unei evaluări a impactului asupra protecției datelor, prezentul Ghid va face referire la prevederile GDPR și la prevederile similare din Legea nr.133/2011.

Totodată, urmează a remarca că GDPR poate fi direct aplicabil oricărei companii stabilite în Moldova dacă prelucrulează date cu caracter personal ale subiecților de date aflați în UE. De asemenea, GDPR poate fi aplicabil în cazul în care o companie înregistrată în Republicii Moldova are înregistrate filiale, reprezentanțe sau orice alte sedii în UE, care prelucrează date cu caracter personal în cadrul activității sale economice, fie când o companie înregistrată în UE are reprezentanțe în Republica Moldova și prelucrează date cu caracter personal în baza instrucțiunilor oferite de compania mamă, elaborate în conformitate cu cerințele GDPR sau când datele personale sunt transferate companiei moldovenești, în calitate de persoană împuternicită de

operator, de la o entitate din UE pentru stocarea sau prestarea unor servicii care implică prelucrarea datelor cu caracter personal.

B. Uniunea Europeană: GDPR

Articolul ce urmează din GDPR se aplică direct tuturor Statelor Membre ale Uniunii Europene.

Art. 35: Evaluarea impactului asupra protecției datelor

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

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

(3) Evaluarea impactului asupra protecției datelor menționată la alineatul (1) 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, menționată la articolul 9 alineatul (1), sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționată la articolul 10; sau

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

(4) 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, în conformitate cu alineatul (1). Autoritatea de supraveghere comunică aceste liste comitetului menționat la articolul 68.

(5) Autoritatea de supraveghere poate, de asemenea, să stabilească și să pună la dispoziția publicului o listă a tipurilor de operațiuni de prelucrare pentru care nu este necesară o evaluare a impactului asupra protecției datelor. Autoritatea de supraveghere comunică aceste liste comitetului.

(6) Înainte de adoptarea listelor menționate la alineatele (4) și (5), autoritatea de supraveghere competentă aplică mecanismul pentru asigurarea coerenței menționat la articolul 63 în cazul în care aceste liste implică activități de prelucrare care presupun furnizarea de bunuri sau prestarea de servicii către subiecții de date sau monitorizarea comportamentului acestora în mai multe state membre ori care pot afecta în mod substanțial libera circulație a datelor cu caracter personal în cadrul Uniunii.

(7) 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 subiecților de date menționate la alineatul (1); 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.

(8) La evaluarea impactului operațiunilor de prelucrare efectuate de operatorii sau de persoanele împuternicite de operatori relevante, se are în vedere în mod corespunzător respectarea de către operatorii sau persoanele împuternicite respective a codurilor de conduită aprobate menționate la articolul 40, în special în vederea unei evaluări a impactului asupra protecției datelor.

(9) Operatorul solicită, acolo unde este cazul, avizul subiecților de date sau al reprezentanților acestora privind prelucrarea prevăzută, fără a aduce atingere protecției intereselor comerciale sau publice ori securității operațiunilor de prelucrare.

(10) Atunci când prelucrarea în temeiul articolului 6 alineatul (1) litera (c) sau (e) are un temei juridic

în dreptul Uniunii sau al unui stat membru sub incidența căruia intră operatorul, iar dreptul respectiv reglementează operațiunea de prelucrare specifică sau setul de operațiuni specifice în cauză și deja s-a efectuat o evaluare a impactului asupra protecției datelor ca parte a unei evaluări a impactului generale în contextul adoptării respectivului temei juridic, alineatele (1)-(7) nu se aplică, cu excepția cazului în care statele membre consideră că este necesară efectuarea unei astfel de evaluări înaintea desfășurării activităților de prelucrare.

(11) Acolo unde este necesar, operatorul efectuează o analiză pentru a evalua dacă prelucrarea are loc în conformitate cu evaluarea impactului asupra protecției datelor, cel puțin atunci când are loc o modificare a riscului reprezentat de operațiunile de prelucrare.

C. Republica Moldova: Legea privind protecția datelor cu caracter personal

Modificările adoptate la Legea nr. 133/2011 prin Legea nr. 175/2021 privind modificarea unor acte normative, în vigoare de la 10 ianuarie 2022, au aceeași abordare ca și GDPR, dar fără instituirea mecanismului pentru asigurarea coerenței în cadrul căruia autoritățile de supraveghere din UE cooperează între ele (art. 63 GDPR).

Articolul 23. Evaluarea impactului asupra protecției datelor

(1) În funcție de natura, domeniul de aplicare, contextul și scopurile prelucrării datelor, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc sporit pentru drepturile și libertățile persoanelor, operatorul efectuează, înaintea prelucrării, evaluarea 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 sporite similare.

(2) La realizarea evaluării impactului asupra protecției datelor, operatorul solicită avizul persoanei responsabile cu protecția datelor, dacă aceasta a fost desemnată.

(3) Evaluarea impactului asupra protecției datelor indicată la alin. (1) se impune mai ales în cazul:

a) evaluării sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv pe crearea de profiluri, și care stă la baza unor decizii automatizate 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 de date care se referă la dezvăluirea originii rasiale sau etnice, a opiniilor politice, a confesiunii religioase sau convingerilor filozofice ori a apartenenței la sindicate, precum și prelucrării de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea ori de date privind viața sexuală sau orientarea sexuală, privind condamnările penale și infracțiunile unei persoane fizice;

c) monitorizării sistematice, pe scară largă, a unei zone accesibile publicului.

(4) Evaluarea conține cel puțin:

a) descrierea sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării datelor, inclusiv, după caz, a interesului legitim urmărit de operator;

b) evaluarea necesității și proporționalității operațiunilor de prelucrare în legătură cu scopurile respective;

c) evaluarea riscurilor pentru drepturile și libertățile subiecților de date menționate la alin. (1), în special originea (sursa), natura, gradul specific de probabilitate a materializării riscului sporit și gravitatea acestui risc. Rezultatul evaluării se ia în considerare la stabilirea măsurilor adecvate care trebuie luate pentru a demonstra că prelucrarea datelor cu caracter personal respectă prezenta lege;

d) măsurile de prevenire a riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu prevederile prezentei legi, luând în considerare drepturile și interesele legitime ale subiecților de date și ale altor persoane interesate.

(5) Operatorul solicită, după caz, avizul în formă scrisă, în formă electronică sau prin utilizarea mijloacelor electronice de comunicație al subiecților de date ori al reprezentanților acestora privind

prelucrarea preconizată, fără a aduce atingere protecției intereselor comerciale sau publice ori securității operațiunilor de prelucrare.

(6) În cazul în care prelucrarea în temeiul art. 5 alin. (5) lit. b) sau d) are un temei juridic prevăzut de actele normative în vigoare, iar dreptul respectiv reglementează operațiunea de prelucrare specifică sau setul de operațiuni specifice în cauză și deja s-a efectuat o evaluare a impactului asupra protecției datelor ca parte a unei evaluări a impactului general în contextul adoptării respectivului temei juridic, prevederile alin. (1)–(3) din prezentul articol nu se aplică, dacă actele normative nu prevăd altfel.

(7) Dacă este necesar, operatorul efectuează o analiză pentru a evalua dacă prelucrarea datelor are loc în conformitate cu evaluarea impactului asupra protecției datelor, cel puțin atunci când are loc o modificare a riscului reprezentat de operațiunile de prelucrare.

(8) CNPDCP 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, în conformitate cu alin. (1).

(9) CNPDCP poate, de asemenea, să stabilească și să pună la dispoziția publicului o listă a tipurilor de operațiuni de prelucrare pentru care nu este necesară o evaluare a impactului asupra protecției datelor.

II. Atribuțiile CNPDCP

A. Lista tipurilor de operațiuni de prelucrare

Odată cu intrarea în vigoare a Legii nr. 175/2021 privind modificarea unor acte normative, CNPDCP, potrivit art. 23 alin. (8) (în redacție nouă) al Legii nr. 133/2011 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, în conformitate cu alin. (1). Astfel, ținând cont de prevederile articolului prenotat, CNPDCP, la data de 31.03.2022, a aprobat Ordinul nr. 27 privind aprobarea Listei tipurilor de operațiuni de prelucrare care fac obiectul cerinței de efectuare a unei evaluări a impactului asupra protecției datelor cu caracter personal¹.

1. Abordarea europeană

<https://ec.europa.eu/newsroom/article29/items/611236>

Se recomandă consultarea *Ghidului privind Evaluarea impactului asupra protecției datelor (DPIA) și stabilirea dacă o prelucrare este „susceptibilă să genereze un risc ridicat” în sensul Regulamentului 2016/679*, revizuit și adoptat în data de 4 octombrie 2017 de către Grupul de lucru Articolul 29 pentru protecția datelor (WP 248).

Pentru a oferi un set mai precis de operațiuni de prelucrare care necesită o DPIA datorită riscului ridicat inerent, ținând seama de elementele speciale ale art. 35 (1) și ale art. 35 (3) a)-c) ale GDPR, la adoptarea la nivel național a listei în conformitate cu art. 35 (4) și Considerentele 71, 75 și 91 și alte referințe ale GDPR la operațiunile de prelucrare „susceptibile să conducă la un risc ridicat”, trebuie a se lua în considerare următoarele nouă criterii:

1. Evaluarea sau scoring-ul, inclusiv profilarea și preconizarea, în special reieșind din „aspecte privind performanța subiectului de date la locul de muncă, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările” (Considerentele 71 și 91 ale GDPR). *Astfel de exemple ar putea include o instituție financiară care își monitorizează clienții prin intermediul unei baze de date de tip credit sau printr-o bază de date destinată spălării banilor sau combaterii finanțării terorismului sau a unei baze de date împotriva fraudei sau a unei companii de biotehnologie care oferă teste genetice direct consumatorilor pentru a evalua și anticipa riscurile referitoare la boală/sănătate sau pentru a crea un profil de comportament sau de marketing bazat pe utilizarea sau navigarea pe site-ul său web.*

¹ Disponibil pe Internet la adresa: <https://datepersonale.md/wp-content/uploads/2022/04/Ordinul-nr.-27-din-31.03.2022.pdf>

2. Procesul decizional automatizat cu efecte legale sau similare semnificative: prelucrare care vizează luarea deciziilor asupra persoanelor vizate care produc „efecte juridice privind persoana fizică” sau care „o afectează în mod similar într-o măsură semnificativă” (art. 35 alin. (3) lit. a) ale GDPR). *Spre exemplu, prelucrarea poate conduce la excluderea sau discriminarea persoanelor fizice.* Prelucrarea cu efect redus sau fără efect asupra persoanelor nu corespunde acestui criteriu specific. Mai multe explicații privind aceste noțiuni sunt oferite în Orientările privind procesul decizional individual automatizat și crearea de profiluri în sensul Regulamentului (UE) 2016/679, revizuit și adoptat în data de 6 februarie 2018 de către Grupul de lucru Articolul 29 pentru protecția datelor (Documentul de lucru 251).

3. Monitorizarea sistematică: prelucrarea folosită pentru a observa, monitoriza sau controla persoanele vizate, incluzând colectarea de date prin rețele sau „monitorizarea sistematică a unei zone accesibile publicului” (art. 35 alin. (3) lit. c) ale GDPR). Acest tip de monitorizare reprezintă un criteriu, deoarece datele cu caracter personal pot fi colectate în situații în care persoanele vizate pot să nu cunoască cine colectează datele și modul în care acestea vor fi utilizate. În plus, poate fi imposibil ca persoanele să nu fie supuse unei astfel de prelucrări în spații (sau zonele publice) accesibile publicului.

4. Date sensibile sau date de natură foarte personală: acestea includ categorii speciale de date cu caracter personal, așa cum sunt definite în art. 9 ale GDPR (*spre exemplu informații privind opiniile politice ale persoanelor fizice*), precum și date cu caracter personal privind condamnările penale sau infracțiunile, așa cum sunt definite în art. 10 ale GDPR. *Un exemplu ar fi un spital care păstrează dosarele medicale ale pacienților sau un detectiv privat care păstrează detaliile infractorilor.* Dincolo de aceste dispoziții din GDPR, unele categorii de date pot fi considerate ca sporind riscul potențial pentru drepturile și libertățile persoanelor. Aceste date cu caracter personal sunt considerate ca fiind sensibile (întrucât acest termen este înțeles în mod obișnuit), deoarece acestea sunt legate de activitățile casnice și private (cum ar fi comunicațiile electronice a căror confidențialitate ar trebui să fie protejată), sau, deoarece afectează exercitarea unui drept fundamental (cum ar fi datele de localizare a căror colectare pune sub semnul întrebării libertatea de circulație) sau nerespectarea caracterului privat al acestora implică, în mod clar, efecte grave în viața de zi cu zi a persoanei vizate (cum ar fi date financiare care ar putea fi utilizate pentru fraudarea sistemelor de plată). În această privință, ar putea fi relevant faptul dacă datele au fost puse deja la dispoziția publicului de către persoana vizată sau de părți terțe. Faptul că datele cu caracter personal sunt puse la dispoziția publicului poate fi considerat un factor în cadrul evaluării, în cazul în care se preconiza că datele urmau să fie utilizate în continuare în anumite scopuri. Acest criteriu poate include, de asemenea, date cum ar fi documentele personale, e-mailurile, jurnalele, dispozitivele electronice de citit echipate cu caracteristici de luare de notițe și informații foarte personale conținute în aplicații de urmărire a sănătății (*spre exemplu, Apple Health, Google Fit*).

5. Date prelucrate pe scară largă: GDPR nu definește ce înseamnă scară largă, însă Considerentul 91 oferă anumite linii directoare. În orice caz, Grupul de Lucru Articolul 29 recomandă luarea în considerare, în special, a următorilor factori pentru a se determina dacă o prelucrare este efectuată pe scară largă:

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

6. Adaptarea/potrivirea sau combinarea seturilor de date, *spre exemplu, provenind de la două sau mai multe operațiuni de prelucrare a datelor efectuate în scopuri diferite și/sau de diverși operatori de date într-un mod care ar depăși așteptările rezonabile ale subiectului de date.*

7. Date privind subiecții de date vulnerabili (Considerentul 75 ale GDPR): prelucrarea acestui tip de date este un criteriu din cauza dezechilibrului de putere crescut între subiecții de date și operatorul de date, ceea ce înseamnă că persoanele ar putea să nu fie în stare să își dea cu ușurință consimțământul sau să se opună prelucrării datelor lor sau să își exercite drepturile. *Subiecții de date vulnerabili pot include copiii (pot fi considerați incapabili să se opună sau să consimtă sau să se opună în mod deliberat la prelucrarea datelor lor), angajații, segmente mai vulnerabile ale populației care necesită protecție*

specială (persoane bolnave, solicitanți de azil sau vârstnici, pacienți etc.) și, în orice caz, poate fi identificat un dezechilibru în relația dintre poziția subiectului de date și operator.

8. Utilizarea inovatoare sau implementarea unor noi soluții tehnologice sau organizaționale cum ar fi combinarea utilizării amprente digitale cu recunoașterea facială pentru îmbunătățirea controlului accesului fizic etc. GDPR clarifică (art. 35 alin. (1) și Considerentele 89 și 91) faptul că utilizarea unei noi tehnologii, definită în „conformitate cu nivelul atins al cunoștințelor tehnologice” (Considerentul 91), poate declanșa necesitatea realizării unei DPIA. Acest lucru se datorează faptului că utilizarea unei astfel de tehnologii poate implica noi forme de colectare și utilizare a datelor, eventual, cu un risc ridicat pentru drepturile și libertățile persoanelor fizice. Într-adevăr, consecințele personale și sociale ale desfășurării unei noi tehnologii pot fi necunoscute. O DPIA va ajuta operatorul să înțeleagă și să abordeze astfel de riscuri. *Spre exemplu, anumite aplicații „Internet of Things” ar putea avea un impact semnificativ asupra vieții cotidiene și a vieții private a persoanelor fizice și, prin urmare, necesită o DPIA.*

9. Atunci când prelucrarea în sine „împiedică persoanele fizice să-și exercite un drept sau să utilizeze un serviciu sau un contract” (art. 22 și Considerentul 91 ale GDPR). Acestea includ operațiuni de prelucrare care vizează permiterea, modificarea sau refuzarea accesului persoanelor fizice la un serviciu sau încheierea unui contract. *Un exemplu ar putea fi atunci când o bancă își verifică clienții prin compararea cu o bază de date a istoriilor de credit pentru a decide acordarea unui împrumut.*

2. Abordarea UK

De asemenea, poate fi utilizat modelul englez de formular, care poate fi accesat pe pagina oficială a Oficiului Comisarului de Informații din Marea Britanie (ICO):

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/#dpia3>

ICO cere realizarea unei DPIA în cazul în care operatorul urmărește:

- utilizarea noilor tehnologii;
- utilizarea datelor de profil sau categoriilor speciale de date cu caracter personal pentru a decide cu privire la accesul la servicii;
- profilarea indivizilor pe scară largă;
- prelucrarea datelor biometrice;
- prelucrarea datelor genetice;
- adaptarea/potrivirea datelor sau combinarea seturilor de date din surse diferite;
- colectarea datelor cu caracter personal dintr-o altă sursă decât de la persoana fizică fără a le oferi o notificare privind confidențialitatea („prelucrare invizibilă”);
- urmărirea locației sau comportamentul persoanelor;
- profilarea copiilor sau marketingul vizat sau serviciile online la acestea;
- procesarea datelor care ar putea pune în pericol sănătatea sau siguranța fizică a persoanei în cazul unei încălcări a securității.

3. Abordarea Germană

Germania furnizează o listă comprehensivă deoarece aceasta este un rezultat comun al negocierilor intensive dintre toate Autoritățile germane de Protecție a Datelor:

https://www.saechsdsb.de/images/stories/sdb_inhalt/DSGVO/DSFA/DSFA_Muss-Liste_V1_20180606.pdf (Traducere neoficială):

- Prelucrarea extinsă a datelor referitoare la asistența socială care fac obiectul secretului profesional chiar dacă acestea nu fac parte din categoria datelor prevăzute la Art. 9 alin. 1 și Art. 10 din GDPR
- Prelucrarea extensivă a datelor personale cu privire la localizarea persoanelor fizice
- Agregarea datelor personale din diverse surse și prelucrarea ulterioară a datelor compilate în cazul în care:
 - ❖ agregarea sau prelucrarea ulterioară se desfășoară pe scară largă;

- ❖ prelucrarea este efectuată pentru scopuri în care nu toate datele care urmează să fie prelucrate sunt colectate de la subiectul de date;
- ❖ include aplicarea unor algoritmi care nu sunt transparenți pentru subiectul de date;
- ❖ producerea de baze de date cu care să se poată lua decizii cu efect juridic asupra persoanei vizate sau care îi pot afecta într-un anumit mod;
- ❖ colectarea optică mobilă a datelor cu caracter personal în domeniul public, unde datele sunt adunate la nivel central de unul sau mai multe sisteme de înregistrări;
- ❖ colectarea și publicarea sau transmiterea datelor cu caracter personal utilizate pentru evaluarea comportamentului și a altor aspecte personale ale subiecților de date și care pot fi utilizate de terți pentru a lua decizii care au efect juridic asupra subiecților de date vizați sau care îi afectează într-un mod similar;
- ❖ prelucrarea datelor cu caracter personal referitoare la comportamentul angajaților care pot fi utilizate pentru evaluarea activității lor de lucru, astfel încât să genereze consecințe juridice pentru subiecții de date sau să-i afecteze în mod semnificativ;
- ❖ crearea de profiluri cuprinzătoare privind interesele, rețeaua de relații personale sau personalitatea subiecților de date;
- ❖ utilizarea inteligenței artificiale pentru prelucrarea datelor cu caracter personal pentru a controla interacțiunea cu subiectul de date sau pentru a evalua aspectele personale ale subiectului de date;
- ❖ utilizarea necorespunzătoare a senzorilor unui dispozitiv mobil deținut de persoanele în cauză sau a semnalelor radio difuzate de la astfel de dispozitive în scopul determinării locului de ședere sau de circulație a persoanelor pe parcursul unei perioade substanțiale de timp;
- ❖ analiza automată a înregistrărilor video sau audio pentru a evalua personalitatea subiectului de date;
- ❖ colectarea de date cu caracter personal pe interfețele dispozitivelor electronice personale care nu sunt protejate împotriva citirii neautorizate, care nu pot fi detectate de persoanele în cauză;
- ❖ crearea de profiluri cuprinzătoare privind mișcarea și comportamentul de cumpărare al subiecților de date;
- ❖ anonimizarea datelor personale speciale în sensul art. 9 din GDPR, în cazul în care datele anonime (dacă există) trebuie divulgate unor părți terțe sau prelucrate nu numai în scopuri statistice interne;
- ❖ prelucrarea datelor cu caracter personal în conformitate cu art. 9 alin. 1 și art. 10 din GDPR, chiar dacă nu sunt prelucrate pe scară largă în sensul art. 35 alin. 3 lit. (b) - în cazul în care datele nu sunt colectate ocazional, dar, și prin utilizarea inovatoare a senzorilor sau a aplicațiilor mobile, și acestea sunt permise și prelucrate de un organ central;
- ❖ prelucrarea datelor cu caracter personal în conformitate cu art. 9 alin. 1 și art. 10 GDPR, chiar dacă nu sunt prelucrate pe scară largă în sensul art. 35 alin. 3 lit. (b) - dacă datele sunt utilizate de furnizorii de noi tehnologii pentru a determina performanța persoanelor în cauză.

B. Consultarea Prealabilă

În principiu, nu este necesar ca operatorul să transmită DPIA către CNPDCP pentru consultarea prealabilă, cu excepția cazurilor menționate în art. 24 al Legii nr. 133/2011, precum și art. 36 al GDPR. În asemenea cazuri, art. 24 al legii prenotate prevede:

Articolul 24. Consultarea prealabilă

(1) Operatorul consultă CNPDCP înainte de prelucrarea datelor dacă evaluarea impactului asupra protecției datelor, prevăzută la art.23, indică faptul că prelucrarea ar genera un risc sporit, iar operatorul consideră că riscul nu poate fi atenuat prin mijloace rezonabile sub aspectul tehnologiilor disponibile și al costurilor implementării.

(2) În cazul în care CNPDCP consideră că prelucrarea prevăzută la alin. (1) ar încălca prezenta lege, în special atunci când riscul nu a fost identificat sau atenuat într-o măsură suficientă de operator, CNPDCP oferă consiliere în scris operatorului și, după caz, persoanei împuternicite de operator în cel mult opt săptămâni de la primirea cererii de consultare, precum și poate utiliza oricare dintre competențele menționate la art. 20. Perioada respectivă poate fi prelungită cu șase săptămâni, ținându-se cont de complexitatea prelucrării prevăzute. CNPDCP informează operatorul și, după caz, persoana

împuțernicită de operator, în termen de o lună de la primirea cererii, cu privire la astfel de prelungire, prezentând detaliat și specific motivele întârzierii. Curgerea acestor perioade poate fi suspendată până când CNPDCP nu a obținut informațiile pe care le-a solicitat în scopul consultării.

(3) În cazul în care operatorul consultă CNPDCP în conformitate cu alin. (1), acesta îi furnizează CNPDCP:

- a) după caz, responsabilitățile corespunzătoare ale operatorului/operatorilor și ale persoanelor împuțernicite de operator implicate în activitățile de prelucrare a datelor, în special pentru prelucrarea în cadrul unui grup de întreprinderi;
- b) scopurile și mijloacele prelucrării preconizate;
- c) măsurile și garanțiile prevăzute pentru protecția drepturilor și libertăților subiecților de date, în conformitate cu prezenta lege;
- d) după caz, datele de contact ale persoanei responsabile cu protecția datelor;
- e) evaluarea impactului asupra protecției datelor, prevăzută la art.23;
- f) alte informații relevante și necesare solicitate suplimentar de CNPDCP.

În practică, aceasta înseamnă că CNPDCP va revizui DPIA (a se vedea mai jos) și va comunica operatorului dacă măsurile întreprinse sunt suficiente pentru diminuarea riscului. În caz contrar, CNPDCP prezintă opinia/recomandările sale.

III. Atribuțiile Operatorului

A. Necesitatea efectuării unei DPIA: risc ridicat pentru drepturile și libertățile persoanelor fizice

Dat fiind faptul că, în majoritatea cazurilor, o DPIA cere eforturi majore, este recomandabil să se verifice cu atenție dacă există o justificare a necesității pentru prelucrarea preconizată/stabilită, reieșind din considerentul dacă o astfel de prelucrare poate duce la un risc ridicat pentru drepturile și libertățile persoanelor fizice. Conform art. 23 alin. (3) al Legii nr.133/2011 și art. 35 al GDPR, o evaluare a impactului asupra protecției datelor trebuie, în special, să fie efectuată în următoarele cazuri:

- a) în cazul evaluării sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv pe crearea de profiluri și care stă la baza unor decizii automatizate care produc efecte juridice privind persoana fizică sau care o afectează, în mod similar, într-o măsură semnificativă;
- b) în cazul prelucrării, pe scară largă, a unor categorii de date care se referă la dezvoltarea originii rasiale sau etnice, a opiniilor politice, a confesiunii religioase sau convingerilor filozofice ori a apartenenței la sindicate, precum și prelucrării de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea ori de date privind viața sexuală sau orientarea sexuală, privind condamnările penale și infracțiunile unei persoane fizice;
- c) în cazul monitorizării sistematice, pe scară largă, a unei zone accesibile publicului.

Conform *Ghidului privind Evaluarea impactului asupra protecției datelor (DPIA) și stabilirea dacă o prelucrare este „susceptibilă să genereze un risc ridicat” în sensul Regulamentului 2016/679*, după cum indică expresia „în special” din teza introductivă a art. 35 (3) din GDPR, aceasta este o listă neexhaustivă. Pot exista operațiuni de prelucrare „cu risc ridicat” care nu sunt cuprinse în această listă, dar prezintă totuși riscuri la fel de mari. Aceste operațiuni de prelucrare ar trebui, de asemenea, să facă obiectul DPIA. Din acest motiv, criteriile prezentate mai jos depășesc uneori o explicație simplă a ceea ce ar trebui înțeles prin cele trei exemple menționate la art. 35 (3) din GDPR și, respectiv, la art. 23 alin. (3) al Legii nr.133/2011.

Potrivit Ghidului menționat, în anumite situații, un operator poate considera că prelucrarea care îndeplinește cel puțin un singur criteriu din cele nouă descrise mai sus la Capitolul II A. 1. necesită efectuarea unei DPIA.

Exemple de prelucrare	Posibile criterii relevante	Este posibil ca DPIA să fie necesară?
Un spital prelucrează datele genetice și datele de sănătate ale pacienților săi (sistemul de informații al spitalului)	Categorii speciale de date cu caracter personal sau date de natură foarte personală. Date privind subiecții de date vulnerabili.	DA
Utilizarea unui sistem de camere pentru a monitoriza comportamentul conducătorilor de vehicule pe autostrăzi. Operatorul intenționează să utilizeze un sistem inteligent de analiză video pentru a identifica vehiculele și pentru a recunoaște în mod automat plăcuțele de înmatriculare	Monitorizare sistematică. Utilizare inovatoare sau implementarea de soluții tehnice sau organizatorice.	
O companie monitorizează în mod sistematic activitatea propriilor angajați, inclusiv monitorizarea angajaților la locul de muncă, navigarea pe Internet etc.	Monitorizare sistematică. Date privind subiecții de date vulnerabili.	
Colectarea de date publice de pe platformele de comunicare socială pentru generarea de profiluri.	Evaluare sau scoring. Date prelucrate pe scară largă	
Un magazin online care utilizează o listă de e-mailuri pentru a trimite abonaților săi raporturile sale zilnice	Niciuna	
Un website de comerț electronic care afișează anunțuri pentru piese de mașini de epocă care implică profiluri limitate bazate pe elemente vizionate sau achiziționate pe site-ul propriu.	Evaluare sau scoring, dar nu sistematic sau extins	NU este necesar

B. Realizarea unei DPIA

Odată ce operatorul constată necesitatea realizării unei DPIA, poate utiliza instrumentul Comisiei Naționale pentru Informatică și Libertăți din Franța (CNIL), care este unul bine structurat și accesibil tuturor (<https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment>). Instrumentul se bazează pe o interfață ușor de utilizat pentru a permite o gestionare simplă a DPIA-urilor. Acesta descrie în mod clar metodologia DPIA pas cu pas și oferă modalități de a înțelege rapid riscurile. Această aplicație poate fi utilizată și implementată de operator, fiind disponibilă în 14 limbi (franceză, engleză, italiană, germană, poloneză, maghiară, finlandeză, norvegiană, spaniolă, cehă, olandeză, portugheză, română și greacă) atât în formă de program executabil, cât și în versiunea web. Codul este de tip open source și poate fi adaptat la software-ul operatorului. Un tutorial video aferent poate fi vizualizat pe <https://www.youtube.com/watch?v=-SdA9L4j0a8>.

Mai mult, informații detaliate pot fi consultate pe <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf>.

Spre deosebire, de exemplu, de Modelul German Standard de Protecție a Datelor, modelul francez se concentrează asupra amenințărilor, riscurilor și măsurilor adecvate în dependență de nivelul de severitate și probabilitate (a se vedea mai jos Capitolul III.B.4).

DPIA trebuie, în principiu, să fie realizată de către operatorii care răspund criteriilor inițiale de determinare a necesității de a realiza o DPIA (a se vede mai sus). Însă, ea este destinată și pentru operatorii de date care doresc să-și demonstreze abordarea și metodologia selectată de către ei (conceptul de responsabilitate, a se vedea art. 24 al GDPR), precum și pentru furnizorii de produse care doresc să demonstreze că soluțiile lor nu încalcă principiul confidențialității datorită unui design care respectă confidențialitatea.

Grupul de Lucru Articolul 29, în Anexa 2 a *Ghidului privind Evaluarea impactului asupra protecției datelor (DPIA), pentru a stabili dacă o prelucrare este „susceptibilă să genereze un risc ridicat” în sensul Regulamentului 2016/679*, propune următoarele **criterii** pe care operatorii de date le pot utiliza pentru a evalua dacă o DPIA sau o metodologie de realizare a unei DPIA este suficient de cuprinzătoare:

- se furnizează o descriere sistematică a prelucrării (art. 35 alin. (7) lit. a) din GDPR / art. 23 alin. (1) lit. a) din Legea nr. 133/2011):
 - se ține cont de natura, domeniul de aplicare, contextul și scopurile prelucrării (Considerentul 90 din GDPR);
 - se înregistrează datele cu caracter personal, destinatarii și perioada pentru care datele cu caracter personal sunt stocate;
 - se furnizează o descriere funcțională a operațiunii de prelucrare;
 - se identifică activele pe care se bazează datele cu caracter personal (hardware, software, rețelele, persoanele, documentele pe suport hârtie sau canalele de transmitere pe suport de hârtie);
 - se ține cont de respectarea codurilor de conduită aprobate (art. 35 alin. (8) din GDPR / în prezent Legea nr. 133/2011 nu conține prevederi referitoare la codurile de conduită);

- se evaluează necesitatea și proporționalitatea operațiunilor de prelucrare în legătură cu scopurile respective (art. 35 (7) b) din GDPR / art. 23 alin. (4) lit. b) din Legea nr. 133/2011):
 - se determină măsurile preconizate în vederea conformării cu legea (art. 35 alin. (7) lit. d) și Considerentul 90 din GDPR / art. 23 alin. (4) lit. d) din Legea nr. 133/2011)), având în vedere:
 - ✓ măsurii care contribuie la proporționalitatea și necesitatea prelucrării în baza:
 - scopurilor determinate, explicite și legitime (art. 5 alin. (1) lit. b) din GDPR / art. 4 alin. (1) lit. b) din Legea nr. 133/2011);
 - legalității prelucrării (art. 6 din GDPR / art. 5 din Legea nr. 133/2011);
 - modului adecvat, pertinent și neexcesiv în ceea ce privește scopul pentru care sînt colectate și/sau prelucrate ulterior (art. 5 alin. (1) lit. c) din GDPR / art. 4 alin. (1) lit. c) din Legea nr. 133/2011);
 - perioadei de stocare limitate (art. 5 alin. (1) lit. e) din GDPR / art. 4 alin. (1) lit. e) din Legea nr. 133/2011);
 - ✓ măsurilor care contribuie la drepturile subiectului de date:
 - informațiilor furnizate persoanei vizate (art. 12, 13 și 14 din GDPR / art. 12 din Legea nr. 133/2011);
 - dreptului de acces (art. 15 din GDPR / art. 13 din Legea nr. 133/2011) și dreptului la portabilitatea datelor (art. 20 din GDPR / dreptului la portabilitatea datelor nu se regăsește în Legea nr. 133/2011);
 - dreptului la rectificare și dreptului la ștergere (art. 16, 17 și 19 din GDPR) / dreptului de intervenție asupra datelor (rectificare, actualizare, blocare, ștergere) - art. 14 din Legea nr. 133/2011);
 - dreptului la opoziție și dreptului la restricționarea prelucrării (art. 18, 19 și 21 din GDPR) / dreptului la opoziție (art. 16 din Legea nr. 133/2011; dreptului la restricționarea prelucrării nu se regăsește în Legea nr. 133/2011);
 - relațiilor cu persoanele împuternicite de operator (art. 28 din GDPR / în prezent Legea nr. 133/2011 nu conține un asemenea articol, dar prevederi ce reglementează această relație se regăsesc în art. 3 la noțiunea „persoană împuternicită de către operator”, art. 29 alin. (2) și art. 30 alin. (2) și (3));
 - garanțiilor pentru transferurile internaționale (Capitolul V din GDPR / Capitolul VII din Legea nr. 133/2011);
 - consultării prealabile (art. 36 din GDPR / art. 24 din Legea nr. 133/2011).

- se gestionează riscurile pentru drepturile și libertățile subiectului de date (art. 35 alin. (7) lit. c) din GDPR /art. 23 alin. (4) lit. c) din Legea nr. 133/2011):
 - *se analizează originea, natura, particularitatea și gravitatea riscurilor (a se vedea Considerentul 84 din GDPR) sau, mai exact, pentru fiecare risc (acces ilegal, modificări nedorite și dispariția datelor) din perspectiva subiecților de date:*
 - ✓ se ține cont de sursele riscurilor (Considerentul 90 din GDPR);
 - ✓ se identifică impactul posibil asupra drepturilor și libertăților subiecților de date în cazul unor evenimente ce includ accesul ilegal, modificările nedorite sau dispariția datelor;
 - ✓ se identifică amenințările care ar putea conduce la accesul ilegal, modificarea nedorită sau dispariția datelor;
 - ✓ se estimează probabilitatea și gravitatea (Considerentul 90 din GDPR);
 - ✓ se determină măsurile preconizate pentru atenuarea respectivelor riscuri (art. 35 alin. (7) lit. d) și Considerentul 90 din GDPR / art. 23 alin. (4) lit. d) din Legea nr. 133/2011);
- sunt implicate părțile interesate:
 - *se solicită avizul persoanei responsabile cu protecția datelor (art. 35 alin. (2) din GDPR / art. 23 alin. (2) din Legea nr. 133/2011);*
 - *se solicită, acolo unde este cazul, avizul subiecților de date sau al reprezentanților acestora (art. 35 alin. (9) din GDPR / art. 23 alin. (5) din Legea nr. 133/2011).*

1. Descrierea sistematică a operațiunilor de prelucrare prevăzute și scopul prelucrării, inclusiv, dacă este cazul, interesul legitim urmărit de operator

Scopul acestei dispoziții este de a obține o imagine de ansamblu clară a operațiunilor de prelucrare a datelor cu caracter personal. Conform documentului de lucru 248 al Grupului de Lucru Articolul 29 (a se vedea mai sus Capitolul II.A.1), DPIA trebuie să respecte următoarele criterii:

- natura, sfera, contextul și scopurile prelucrării sunt luate în considerare (considerentul 90);
De ex. camerele de supraveghere sunt instalate la intrarea într-o sală de sport pentru prevenirea furtului.
- datele cu caracter personal care sunt înregistrate, destinatarii și perioada pentru care vor fi stocate datele cu caracter personal;
De ex. datele angajaților și clienților prelucrate prin intermediul camerelor de supraveghere vor fi stocate timp de 30 de zile.
- este furnizată o descriere funcțională a operațiunii de prelucrare;
De ex. datele înregistrate prin intermediul camerelor de supraveghere vor fi utilizate în cazul infracțiunilor.
- sunt identificate produsele tehnologice utilizate la prelucrarea datelor cu caracter personal (hardware, software, rețele, persoane, canale de transmisie);
De ex. camerele, software de video management folosite.
- se ține cont de respectarea codurilor de conduită aprobate (art. 35 alin. (8) GDPR / în redacția actuală a Legii nr. 133/2011 nu sunt prevăzute codurile de conduită)

2. Evaluarea necesității și proporționalității operațiunilor de prelucrare în raport cu scopurile

Scopul acestei dispoziții este de a asigura respectarea principiilor de protecție a vieții private. Conform documentului de lucru 248 al Grupului de Lucru Articolul 29 (a se vedea mai sus Capitolul II.A.1), DPIA trebuie să respecte următoarele criterii:

Măsurile preconizate pentru conformarea cu GDPR/Legea nr. 133/2011 sunt determinate, ținând cont de:

- măsurilor care contribuie la proporționalitatea și necesitatea prelucrării în baza:
 - scopului/-urilor determinat/-e, explicit/-e și legitim/-e (art. 5 alin. (1) lit. b) GDPR / art. 4 alin. (1) lit. b) din Legea nr. 133/2011);
De ex. pentru prevenirea furturilor.
 - legalității prelucrării (art. 6 GDPR / art. 5 din Legea nr. 133/2011);
De ex. un contract pentru clienți sau interesul legitim.
 - modului adecvat, pertinent și neexcesiv în ceea ce privește scopul pentru care sînt colectate și/sau prelucrate ulterior [art. 5 alin. (1) lit. c) din GDPR / art. 4 alin. (1) lit. c) din Legea nr. 133/2011];
De ex. limitat la zona de intrare, alte zone nu se supraveghează.
 - duratei de stocare limitată (art. 5 alin. (1) lit. e) din GDPR / art. 4 alin. (1) lit. e) din Legea nr. 133/2011);
De ex. 30 de zile.
- măsurilor care contribuie la respectarea drepturilor subiecților de date:
 - informații furnizate subiectului de date (art. 12, 13 și 14 din GDPR / art. 12 din Legea nr. 133/2011);
De ex. informație pe site, panou de informații.
 - dreptul de acces (art. 15 din GDPR / art. 13 din Legea nr. 133/2011) și dreptul la portabilitatea datelor (art. 20 din GDPR / dreptul la portabilitatea datelor nu se regăsește în Legea nr. 133/2011);
De ex. punerea la dispoziție a unui formular.
 - dreptul la rectificarea și dreptul la ștergere (art. 16, 17 și 19 din GDPR) / dreptul de intervenție asupra datelor (rectificare, actualizare, blocare, ștergere) - art. 14 din Legea nr. 133/2011);
De ex. punerea la dispoziție a unui formular.
 - dreptul la opoziție și dreptul la restricționarea prelucrării (art. 18, 19 și 21 din GDPR) / dreptul la opoziție (art. 16 din Legea nr. 133/2011; dreptul la restricționarea prelucrării nu se regăsește în Legea nr. 133/2011);
De ex. punerea la dispoziție a unui formular.
- relațiile cu persoanele împuternicite de operator (art. 28 GDPR / art. 3 noțiunea „persoană împuternicită de către operator”, art. 29 alin. (2) și art. 30 alin. (2) și (3) din Legea nr. 133/2011);
De ex. verificarea contractelor cu companiile de instalare și menținere.
- garanțiile privind transferul (transferurile) internațional (Capitolul V din GDPR și Capitolul VII din Legea nr. 133/2011);
De ex. date din cloud.
- consultația prealabilă (art. 36 din GDPR / art. 24 din Legea nr. 133/2011).

3. Evaluarea riscurilor la adresa drepturilor și libertăților subiecților de date

Scopul acestei prevederi este de a înțelege bine criteriile care contribuie la securitate, precum și cauzele și consecințele riscurilor. Conform documentului de lucru 248 al Grupului de Lucru Articolul 29 (a se vedea mai sus Capitolul II.A.1), o DPIA trebuie să respecte următoarele criterii:

- | |
|---|
| <input type="checkbox"/> originea, natura, specificitatea/particularitatea și gravitatea riscurilor (a se vedea Considerentul 84) sau, mai exact, pentru fiecare risc din perspectiva persoanelor vizate
<i>de ex. acces nelegitim, modificări nedorite și dispariția datelor.</i> |
| <input type="checkbox"/> sursele de risc sunt luate în considerare (considerentul 90 din GDPR)
<i>de ex. uși neînchise, acces nerestricționat la baza de date.</i> |
| <input type="checkbox"/> impactele potențiale asupra drepturilor și libertăților subiecților de date sunt identificate în cazul unor evenimente care includ accesul nelegitim, modificări nedorite și dispariția datelor
<i>de ex. publicarea imaginilor video din sala de sport a unei persoane aflate pe foaie de boală.</i> |
| <input type="checkbox"/> amenințări care ar putea conduce la accesul ilegal, modificarea nedorită sau dispariția datelor |
| <input type="checkbox"/> estimarea probabilității și gravității (considerentul 90 din GDPR)
<i>de ex. accesul angajaților la datele cu caracter personal prelucrate.</i> |

Conform instrumentului DPIA elaborat de CNIL acest criteriu poate fi neglijabil limitat, semnificativ sau maxim. Pentru detalii a se vedea pagina 5 suportul informațional a instrumentului DPIA francez pe <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf>.

4. Măsurile prevăzute pentru abordarea riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele pentru asigurarea protecției datelor cu caracter personal și pentru a demonstra conformitatea cu legea ținând cont de drepturile și interesele legitime ale subiecților de date

Articolele 5, 12, 25 și 32 ale GDPR / art. 30 din Legea nr. 133/2011 prevăd cerințe esențiale privind asigurarea securității prelucrării datelor cu caracter personal.

Suplimentar, GDPR impune o procedură de revizuire periodică, analiză și evaluare a eficacității măsurilor tehnice și organizatorice (art. 32 alin. (1) lit. (d) din GDPR). GDPR oferă posibilitatea evaluării procedurilor bazate pe IT în codurile de conduită și prin mecanisme de certificare (art. 40-43 ale GDPR). Articolul 5 al GDPR / art.4 din Legea nr. 133/2011 stabilește principiile de bază pentru prelucrarea datelor cu caracter personal: datele cu caracter personal sunt prelucrate în mod legal, corect și transparent, colectate în scopuri precise, explicite și legitime, bazate pe date exacte, protejate împotriva pierderii, distrugerii sau deteriorării și într-un fel care asigură integritatea și confidențialitatea acestora.

Recomandăm consultarea Modelului Standard de Protecție a Datelor (în continuare - SDM), autorizat pentru publicare în noiembrie 2016, în urma Conferinței autorităților independente de protecție a datelor a Federației și Landurilor Germaniei. Chiar dacă scopul adoptării SDM a fost armonizarea cerințelor diferitor legi ale Landurilor privind protecția datelor, acesta este pe deplin conform cu GDPR.

SDM oferă mecanisme adecvate pentru a conforma măsurile tehnice și organizatorice la cerințele legale ale GDPR. Pentru a atinge acest scop, SDM structurează cerințele legale în sapte obiective de protecție a datelor (https://www.saechsdsb.de/images/stories/sdb_inhalt/schwerpunkt/SDM-Methodology_V1.0.pdf):

a) Minimizarea datelor

"Minimizarea datelor" este menționată în mod explicit ca principiu general în Articolul 5 alineatul (1) litera (c), precum și în art. 25 din GDPR / art. 4 alin. (1) lit. c) din Legea nr. 133/2011. Datele cu caracter personal sunt adecvate, pertinente și neexcesive în ceea ce privește scopul pentru care sînt colectate și/sau prelucrate ulterior.

Scopul de protecție prin minimizarea datelor poate fi realizat prin:

- Reducerea categoriilor de date colectate ale subiectului de date (de ex. nu se colectează patronimicul dacă nu este necesar)
- Reducerea opțiunilor de prelucrare în raport cu operațiunile de prelucrare, (de ex. lista definitivă a destinatarilor)
- Reducerea posibilităților de cunoaștere a datelor existente (de ex. acces limitat)
- Preferințe pentru operațiuni automatizate de prelucrare (în procese non-decizionale), care fac inutilă utilizarea datelor prelucrate și limitează posibilitatea imixtunii, în comparație cu procesele controlate prin dialog (extragerea automată a unui set limitat de date dintr-o bază de date conform unor condiții clar definite)
- Implementarea metodelor de rutină automate de blocare și ștergere; procedurile de pseudonimizare și anonimizare
- Reguli pentru a controla procesele pentru schimbarea procedurilor (de ex. competențe definite).

b) Disponibilitatea

Principiul disponibilității este inclus nemijlocit în art. 32 alin. (1) lit. (b) și (c) al GDPR în contextul securității prelucrării datelor. El este, de asemenea, prezent în art. 5 alin. (1) lit. (e) din GDPR / art. 4 alin. (1) lit. e) din Legea nr. 133/2011 ca o condiție prealabilă pentru identificarea persoanei vizate. Acesta asigură disponibilitatea datelor pentru scopul respectiv, atât timp cât acest scop rămâne valabil. Principiul se aplică obligațiilor de informare și de acces al subiectului de date (art. 13 și 15 din GDPR /art. 12 și 13 din Legea nr. 133/2011).

Măsurile tipice de garantare a disponibilității sunt:

- Pregătirea backup-urilor de date, stărilor de proces, configurațiilor, structurilor de date, istoriilor tranzacțiilor etc., în conformitate cu un concept testat,
- Protecția împotriva influențelor externe (malware, sabotaj, forță majoră)
- Documentarea seturilor de date prelucrate,
- Redundanța hardware-ului și software-ului, precum și a infrastructurii,
- Implementarea strategiilor de reparare și a proceselor alternative,
- Reguli de înlocuire a angajaților absenți.

c) Integritatea

"Integritatea" este menționată în mod explicit ca principiu general în art. 5 alin. (1) lit. (f) al GDPR, precum și în art. 32 al GDPR / art. 30 alin. (1) din Legea nr. 133/2011. Aceasta se referă, pe de o parte, la cerința conform căreia procesele și sistemele tehnologiei informației respectă în mod continuu specificațiile care au fost determinate pentru îndeplinirea funcțiilor propuse. Pe de altă parte, integritatea înseamnă că datele care urmează să fie prelucrate rămân intacte, complete și actualizate.

Măsurile tipice pentru a garanta integritatea sau pentru a evalua o încălcare a integrității sunt:

- Restricționarea permisiunilor de scriere și modificare,
- Utilizarea sigiliilor și a semnăturilor electronice în prelucrarea datelor în conformitate cu un concept criptografic,
- Atribuirea documentată a drepturilor și a rolurilor,
- Descrierea proceselor pentru menținerea actualității datelor,
- Specificarea comportamentului nominal al procesului și a testelor periodice pentru determinarea și documentarea funcționalității, riscurilor, lacunelor de siguranță și a efectelor secundare ale proceselor,
- Specificarea comportamentului nominal al fluxului de lucru sau a proceselor și testarea periodică pentru a determina starea actuală a proceselor.

d) Confidențialitatea

Obligația de a păstra confidențialitatea rezultă în special din art. 5 alin. (1) lit. (f), art. 32 alin. (1) lit. (b) și art. 38 alin. (5) (obligația de confidențialitate a responsabilului cu protecția datelor), art. 28 alin. (3) lit. (b) (obligația de confidențialitate a persoanei împuternicite de operatorul de date) din GDPR / art. 29 din Legea nr. 133/2011. Aceasta asigură protecția împotriva prelucrării neautorizate și ilegale. O încălcare a confidențialității în general constituie o prelucrare a datelor cu caracter personal care nu corespunde prevederilor legale.

Măsurile tipice de garantare a confidențialității sunt:

- Definirea conceptului de drepturi și roluri în conformitate cu principiul necesității pe baza gestionării identității de către operator,
- Implementarea unui proces de autentificare securizat,

- Limitarea personalului autorizat la cei care sunt responsabili în mod verificabil (local, profesional), calificați, fiabili (dacă este necesar cu autorizație de securitate) și aprobați oficial și cu care nu pot apărea conflicte de interese în exercitarea atribuțiilor lor,
- Specificarea și controlul utilizării resurselor aprobate, în special a canalelor de comunicare,
- Spații specifice (clădiri, încăperi) echipate pentru procedură,
- Specificarea și controlul procedurilor organizatorice, a reglementărilor interne și a obligațiilor contractuale (obligația de a păstra secretul datelor, acordurile de confidențialitate etc.)
- Criptarea datelor stocate sau transferate, precum și stabilirea proceselor de gestionare și protecție a informațiilor criptografice (concept criptografic)
- Protecția împotriva influențelor externe (spionaj, hacking).

e) Necorelarea (Unlinkability)

Obligația de prelucrare a datelor numai în scopurile pentru care au fost colectate este inclusă în GDPR prin intermediul principiului limitării scopului de la art. 5 alin. (1) lit. b) / art. 4 alin. (1) din Legea nr. 133/2011. În cazul prelucrării datelor pe bază de consimțământ, din art. 7 alin. (4) din GDPR rezultă că consimțământul poate fi nevalabil dacă acesta nu este necesar pentru îndeplinirea scopului. O măsură tipică pentru necorelare este, de exemplu, pseudonimizarea menționată la art. 40 alin. (2) lit. (d) din GDPR / depersonalizarea menționată la art. 3 și art. 31 din Legea nr. 133/2011.

Măsurile tipice de asigurare a necorelării sunt:

- Restricționarea drepturilor de prelucrare, utilizare și transfer,
- În ceea ce privește programarea, omiterea sau închiderea interfețelor în procedurile și componentele procedurilor,
- Dispoziții de reglementare pentru interzicerea backdoors („ușilor secrete”), precum și pentru stabilirea reviziilor de asigurare a calității pentru respectarea standardelor de dezvoltare software,
- Separarea în limitele organizatorice / departamentale,
- Separarea prin intermediul conceptelor de rol cu drepturi de acces diferențiate pe baza unei gestionări a identității de către autoritatea responsabilă și a unei metode de autentificare sigură,
- Aprobarea managementului de identitate controlat de utilizator de către persoana împuternicită de către operator,
- Utilizarea pseudonimelor specifice scopului, serviciilor de anonimizare, a acreditărilor anonime, prelucrarea datelor pseudonimizate sau anonimizate,
- Proceduri reglementate pentru modificarea scopului.

f) Transparența

Principiul transparenței este prevăzut la art. 5 alin. (1) litera (a) din GDPR. Acesta este reflectat ca principiu fundamental al legislației privind protecția datelor în numeroasele reglementări ale GDPR. În special obligațiile de informare și de acces iau în considerare acest principiu.

Măsurile tipice de garantare a transparenței sunt:

- Documentarea procedurilor, incluzând în special procesele de lucru, stocurile de date, fluxurile de date și sistemele IT utilizate, procedurile de operare, descrierea procedurii, interacțiunea cu alte proceduri,
- Documentația de testare, de aprobare și, după caz, de verificare prealabilă a unor noi proceduri sau a procedurii modificate,
- Documentarea contractelor cu angajații interni; contracte cu prestatori externi de servicii și cu terți, din care sunt colectate sau transferate date; planuri de distribuție a afacerilor, misiuni de responsabilitate internă,
- Documentarea consimțământului și obiecțiilor,
- Logarea accesului și a modificărilor,
- Verificarea surselor de date (autenticitate),
- Versiunea de control,

- Documentarea procedurilor de prelucrare prin intermediul protocoalelor pe baza unui concept de logare și evaluare,
- Examinarea drepturilor subiectului de date vizat în conceptul de logare și evaluare.

g) Dreptul de intervenție (Intervenability)

Dreptul de intervenție al subiectului de date vizat derivă nemijlocit din prevederile privind rectificarea, blocarea, ștergerea și dreptul de opoziție (art. 16-17 din GDPR/art. 14 și art. 16 din Legea nr. 133/2011).

Măsurile tipice de garantare a dreptului de intervenție sunt:

- Opțiuni diferențiate pentru consimțământ, retragere și obiecție,
- Crearea câmpurilor de date necesare, de ex. pentru blocarea indicatorilor, notificări, consimțăminte, obiecții, dreptul la replică,
- Manipularea documentată a disfuncționalităților, metodelor de rezolvare a problemelor și a modificărilor procedurii, precum și a măsurilor de protecție a securității IT și a protecției datelor,
- Dezactivarea opțiunilor pentru funcțiile individuale fără a afecta întregul sistem,
- Implementarea interfețelor standardizate de interogare și de dialog pentru persoanele în cauză pentru a evalua și /sau a executa cererile,
- Trasabilitatea activităților operatorului pentru garantarea drepturilor subiectului de date,
- Stabilirea unui punct unic de contact (SPoC) pentru subiecții de date,
- Posibilități operaționale de a compila, bloca și șterge toate datele stocate cu privire la o singură persoană.

h) Nivelul de protecție

Măsurile necesare pentru atingerea obiectivelor de protecție sunt rezultatul unei analize de la caz la caz și depind de nivelul de protecție. Spre deosebire de standardele de securitate a informațiilor care se concentrează pe protecția organizației care prelucrează date, Modelul Standard de Protecție a Datelor (SDM) ia în considerare perspectiva subiectului de date și exercitarea drepturilor sale fundamentale. Pentru specificarea nivelului de protecție în conformitate cu SDM, nivelul interferenței pe care îl reprezintă prelucrarea datelor de către organizație față de subiectul de date este decisiv.

Pentru a putea evalua nivelul necesar de asigurare a securității informațiilor, de regulă, se va estima cantitatea de daune și probabilitatea de apariție și se va evalua riscul care rezultă din acestea. Cu toate acestea, protecția (drepturilor fundamentale) persoanelor nu este în centrul acestei metode. Pentru a putea evalua semnificația riscurilor legate de dreptul la autodeterminare informațională și nivelul individual de protecție care rezultă dintr-o procedură, nivelul de interferență asupra drepturilor fundamentale trebuie evaluat printr-o procedură. O măsură pentru nivelul de interferență este, printre altele, scopul prelucrării datelor care este determinat de temeiul juridic corespunzător, nivelul de protecție, durata stocării, tipul și numărul de posibili destinatari ai datelor prelucrate. Astfel, aplicarea SDM poate duce la concluzia că nivelul de protecție pentru un proces de afaceri nu corespunde nivelului de protecție necesar pentru a asigura drepturile fundamentale ale subiecților de date.

SDM diferențiază cele trei categorii de protecție "normal", "ridicat" și "foarte ridicat" pentru procedurile de prelucrare a datelor cu caracter personal.

Nivelul de protecție categoria „normal”

Întrucât orice prelucrare a datelor cu caracter personal reprezintă o ingerință în drepturile fundamentale ale subiectului de date, nivelul de protecție nu poate - în conformitate cu SDM - să nu fie niciodată sub "normal". Din acest motiv, trebuie să se presupună că fiecare procedură care implică prelucrarea datelor cu caracter personal necesită cel puțin un nivel normal de protecție. În consecință, un nivel mai scăzut de protecție poate exista numai atunci când prelucrarea datelor nu implică date cu caracter personal.

Nivelul de protecție categoria „ridicat”

Următoarele exemple de scenarii de prelucrare implică un nivel de interferență care poate duce la un nivel mai ridicat de protecție:

- Prelucrarea datelor personale nemodificabile, care, pentru tot parcursul vieții, pot servi drept o ancorare pentru profilare, adică pot fi atribuite unei persoane fizice identificabile (de exemplu date biometrice, date genetice);
- Diseminarea datelor care identifică în mod concret, date cu nivel ridicat de interconexiune (de exemplu, numărul de asigurare de sănătate valabil pe toată durata de viață a subiectului de date, IDNP);
- Lipsa de transparență justificată din punct de vedere juridic sau în alt mod pentru subiecții de date în ceea ce privește procedurile de prelucrare a datelor cu caracter personal (de exemplu, securitatea statului, valorile estimate în scoring);
- Prelucrarea datelor în cadrul procedurilor cu potențiale consecințe financiare grave pentru subiectul de date
- Prelucrarea datelor în cadrul procedurilor cu consecințe potențiale asupra statutului / reputației subiectului de date,
- Prelucrarea datelor într-o procedură cu potențiale consecințe asupra integrității fizice a subiectului de date,
- Prelucrarea datelor care, în mod realist, pot avea un impact asupra exercitării drepturilor fundamentale ale unui număr mare de subiecți de date (de exemplu, în cazul unei supravegheri video pe scară largă)
- Riscul de discriminare, stigmatizare (de exemplu, prin intermediul algoritmilor, realizarea netransparentă a deciziilor referitoare la subiectul de date);
- Intervenția specifică în zonele de protecție a vieții unui subiect de date.

Nivelul de protecție categoria „foarte ridicat”

Un nivel foarte ridicat de protecție este necesar pentru prelucrarea în care un subiect de date este direct și cu importanță vitală dependent de deciziile sau serviciile unei organizații. Riscurile suplimentare apar atunci când efectele unei prelucrări nu pot fi aduse la cunoștința subiectului de date.

De ex. prelucrarea datelor privind maladii serioase, cazierul judiciar

5. Implicarea părților interesate

Scopul acestei dispoziții este de a implica părțile interesate. Conform documentului de lucru 248 al Grupului de Lucru Articolul 29 (a se vedea mai sus Capitolul II.A.1), DPIA trebuie să respecte următoarele criterii:

se solicită avizul Persoanei responsabile cu protecția datelor (DPO) (art. 35 alin. (2) / art. 23 alin. (2) din Legea nr. 133/2011);

se solicită opiniile subiecților de date sau ale reprezentanților acestora (art. 35 alin. (9) / art. 23 alin. (5) din Legea nr. 133/2011).

Operațiunile de prelucrare a datelor cu caracter personal prezintă anumite riscuri inerente pentru drepturile persoanelor fizice. Datele cu caracter personal pot fi pierdute, divulgate unor părți neautorizate sau prelucrate în mod ilegal. În mod evident, riscurile variază în funcție de natura și amploarea prelucrării. Din aceste considerente, DPIA este un instrument care ajută operatorii de date să realizeze operațiuni de prelucrare a datelor cu caracter personal în corespundere cu legislația în vigoare în domeniul protecției datelor cu caracter personal și cu respectarea vieții private a subiecților de date, referindu-se la prelucrarea datelor cu caracter personal care este de natură să genereze un risc ridicat pentru drepturile și libertățile subiecților de date.