Anexa Nr. 1 a Raportului de Misiune

Numele expertului	Tino Naumann
Numărul activității	2.9
Datele misiunii	19/11/2018-23/11/2018
Denumirea Anexei	Manual privind Evaluarea Impactului asupra Protecției Datelor (DPIA) *Denumirea in Engleaza:* DPIA Manual

Twinning project
"Capacity Building of the National Centre for Personal Data Protection
of the Republic of Moldova"
Twinning MD 13 ENPI JH0317 (MD/29)

Articolul 40 al proiectului de Lege privind protecția datelor cu caracter personal

Evaluarea impactului asupra datelor cu caracter personal (DPIA)

Manual

Cuprins

I. Conținut

A. Introducere

Analiza DPIA este un instrument care este conceput pentru evaluarea respectării obligațiilor de protecție a datelor de către companii și organele publice și pentru a identifica eventualele riscuri și strategii de reducere a lor. O evaluare DPIA ar trebui, în mod ideal, să fie finalizată în faza de proiectare a unui nou sistem sau program și apoi revizuită atunci când cerințele privind programul și obligațiile legale suferă schimbări.

Pentru a spori respectarea Legii aplicabile privind protecția datelor, în cazul în care operațiunile de prelucrare pot duce la un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul ar trebui să fie responsabil de realizarea unei DPIA pentru a evalua, în special, originea, natura, particularitatea și gravitatea acestui risc.

Astfel de tipuri de operațiuni de prelucrare pot fi acelea care, în special, implică utilizarea de noi tehnologii sau sunt de un tip nou și în cazul în care DPIA 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 DPIA înainte de prelucrare, pentru a evalua probabilitatea și gravitatea specifică riscului ridicat, luând în considerare natura, scopul, contextul și scopurile prelucrării și sursele de risc. Această DPIA ar trebui să includă, în special, măsurile, garanțiile și mecanismele prevăzute pentru micșorarea acestui risc, asigurarea protecției datelor cu caracter personal și demonstrarea conformității cu prezentul Regulament.

În cazul în care o DPIA indică faptul că operațiunile de prelucrare implică un risc ridicat pe care operatorul n-îl poate reduce prin măsuri adecvate în ceea ce privește tehnologia disponibilă și costurile de punere în aplicare, o consultare prealabilă a autorității de supraveghere trebuie să aibă loc înainte de prelucrare.

B. UE: GDPR

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

> Articolul 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 persoane vizate 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 persoanelor vizate 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 persoanelor vizate 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. Legea Moldovenească

Modificarea elaborată are aceeași abordare ca și GDPR, dar din motive evidente, fără dispozițiile privind mecanismul de asigurare a coerenței al GDPR, precum și al Comitetului.

Articolul 40. Evaluarea impactului asupra datelor personale

(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 subiecților de date, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor personale. 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 de protecția datelor, dacă acesta a fost desemnat.

(3) Evaluarea impactului asupra protecției datelor menționată la alin. (1) se impune, în special, în cazul:

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

b) prelucrării pe scară largă a unor categorii speciale de date, menționată la art. 9 alin. (1);

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

(4) Centru stabilește 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).

(5) Centrul 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.

(6) 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 menționată în alin. (1);

d) măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor personale și să demonstreze conformitatea cu dispozițiile legislației, luând în considerare drepturile și interesele legitime ale subiecților de date și ale altor persoane interesate.

(7) La evaluarea impactului operațiunilor de prelucrare efectuate de operatori sau de persoanele împuternicite de operatori, se are în vedere respectarea de către aceștia a actelor normative în domeniul protecției datelor personale inclusiv a codurilor de conduită, după caz.

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

(9) Atunci când prelucrarea în temeiul art. 5 alin. (1) lit. c) și e) are un temei juridic care reglementează operațiunea de prelucrare specifică sau setul de operațiuni specifice în cauză și doar cu condiția că s-a efectuat o evaluare a impactului asupra protecției datelor ca parte a unei evaluări a impactului general în contextul adoptării respectivului temei juridic, alineatele (1) - (7) nu se aplică.

(10) 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.

II. Atribuțiile CNPDP

A. Lista tipurilor de operațiuni de prelucrare

Odată cu intrarea în vigoare a Legii modificate, CNPDCP va putea (în conformitate cu alin. 5) să stabilească și să facă publică lista tipurilor de operațiuni de prelucrare pentru care nu este necesară o evaluare a impactului asupra protecției datelor personale. Conform alin. 4 Centrul "stabilește și publică lista tipurilor de operațiuni de prelucrare care fac obiectul cerinței de efectuare a unei evaluări a impactului asupra protecției datelor personal". În acest scop, CNPDCP poate revizui documentele existente:

1. Abordarea europeană

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

În primul rând, există documentul de lucru 248 „**Orientările** Grupului de lucru al articolului 29 **privind evaluarea impactului** asupra **protecției datelor**(EIPD)". Aceasta recomandă să se ia în considerare următoarele criterii pentru lista care urmează să fie adoptată la nivel național în conformitate cu Articolul 35 alineatul (4):

- Evaluarea sau scoring, inclusiv profilarea și preconizarea, în special din „aspecte privind performanța persoanei vizate la locul de muncă, situația economică, starea de sănătatea, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările" (Considerentele 71 și 91). Astfel de exemple ar putea include o instituție financiară care își monitorizează clienții printr-o bază de date de tip credit sau printr-o bază de date destinată spălării banilor sau combaterea 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 prezice riscurile pentru boală/sănătate sau pentru a crea un profil de comportament sau de marketing bazat pe utilizarea sau navigarea pe site-ul său web.

- Proces 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 (3) a)). Spre exemplu, prelucrarea poate conduce la excluderea sau discriminarea persoanelor. Prelucrarea cu efect redus sau fără efect asupra persoanelor nu corespunde acestui criteriu specific. Mai multe explicații privind aceste noțiuni vor fi oferite prin viitorul Ghid al Grupului de Lucru Articolul 29 privind profilarea.
- Monitorizare sistematică: prelucrare folosită pentru a observa, monitoriza sau controla persoanele vizate, incluzând colectarea de data prin rețele sau „monitorizarea sistematică a unei zone accesibile publicului” (art. 35 (3) c)) 15 . Acest tip de monitorizare reprezintă un criteriu deoarece datele cu caracter personal pot fi colectate în situații în care persoanele vizate pot să nu fie conștiente de 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 prelucrării în spațiul (sau zonele publice) accesibile publicului.
- Date sensibile: acestea includ categorii speciale de date cu caracter personal așa cum sunt definite în art. 9 (spre exemplu informații privind opiniile politice al persoanelor fizice), precum și date cu caracter personal privind condamnările penale sau infracțiuni, Un exemplu ar fi un spital general care păstrează dosarele medicale ale pacienților sau un anchetator privat care păstrează detaliile infractorilor. Dincolo de aceste prevederi ale RGPD, anumite categorii de date pot fi considerate că ar crește riscul posibil pentru drepturile și libertățile persoanelor cum ar fi comunicațiile electronice, datele de localizare, datele financiare care ar pute fi folosite pentru fraudarea plăților). În acest sens, ar putea fi relevant dacă datele au fost deja puse la dispoziția publicului de către persoana vizată sau de terți. Faptul că datele cu caracter personal sunt disponibile în mod public poate fi considerat un factor în evaluarea dacă datele se preconizează a fi utilizate în continuare în anumite scopuri. Acest criteriu poate include, de asemenea, informația prelucrată de o persoană fizică în cursul activităților pur personale sau casnice (cum ar fi servicii de cloud computing pentru gestionarea documentelor personale, e-mailurile, jurnalele, notele de la cititorii electronici echipate cu funcții de notare și informații foarte personale conținute în aplicațiile de log), divulgarea sau prelucrarea cărora în scopuri diferite decât cele casnice ar putea fi percepută ca fiind foarte intruzivă.
- Date prelucrate pe scară largă: RGPD 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 16:
    - numărul persoanelor vizate, ori un număr exact ori un procent din populația relevantă;
    - volumul datelor și/sau gama de elemente diferite de date în curs de prelucrare;
    - durata sau permanența activității de prelucrare a datelor;
    - suprafața geografică a activității de prelucrare
- 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 persoanei vizate.
- Date privind persoanele vizate vulnerabile (Considerentul 75): prelucrarea acestui tip de date este un criteriu din cauza dezechilibrului de putere crescut între persoanele vizate 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. Spre exemplu, angajații ar întâmpina des dificultăți în a se opune prelucrării realizate de către angajator atunci când aceasta este necesar pentru gestionarea resurselor umane, De asemenea, pot fi considerați incapabili să se opună sau să consimtă sau să se opună în mod deliberat la prelucrarea datelor lor. Aceasta include, de asemenea, segmentele mai vulnerabile ale populației cum ar fi (persoane bolnave, solicitanți de azil sau

vârstnici, pacienți etc.) și, în orice caz, poate fi identificat un dezechilibru în relația dintre poziția persoanei vizate și operator.

- Utilizare inovatoare sau implementarea unor noi soluții tehnologice sau organizaționale cum ar fi combinarea utilizării amprentei digitale cu recunoașterea facială pentru îmbunătățirea controlului accesului fizic etc. RGPD clarifică (art. 35 (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 utilizarea 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.
- Transferul transfrontalier al datelor în afara Uniunii Europene (considerentul 116), luând în considerare, printre altele, țara sau țările de destinație, posibilitatea transferurilor ulterioare sau probabilitatea transferurilor în baza unor derogări pentru situațiile specifice stabilite de GDPR
- 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). Acestea includ operațiuni de prelucrare care vizează permiterea, modificarea sau refuzarea accesului persoanelor fizice la un serviciu încheierea unui contract. Un exemplu ar putea fi atunci când o bancă își verifică clienții prin compararea cu o bază de date referitoare la credit pentru a decide acordarea unui împrumut.

2. Abordarea UK

De asemenea, puteți utiliza lista clară afișată a ICO ca model:

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

• utilizarea noilor tehnologii;
• utilizarea datele de profil sau categoriilor speciale de date pentru a decide cu privire la accesul la servicii;
• profilarea indivizilor pe scară largă;
• prelucrarea datelor biometrice;
• prelucrarea datelor genetice;
• 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 de către Expertul pe termen scurt) :

- Prelucrarea extinsă a datelor referitoare la asistența socială care fac obiectul secretului profesional sau specific profesional chiar dacă acestea nu sunt date în conformitate cu Articolul 9 aliniatul 1 și 10 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 pentru scopuri pentru 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 în mod similar;
    - 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 similar 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 articolului 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 a GDPR, chiar dacă nu pe o scară largă în sensul Art. 35 alin. 3 lit. (b) - în cazul în care datele sunt colectate nu numai ocazional și prin utilizarea inovatoare a senzorilor sau a aplicațiilor mobile, și acestea sunt primite 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 pe o 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 CNPDP pentru consultarea prealabilă, cu excepția cazurilor menționate în articolul 41 al proiectului de amendament la Legea Republicii Moldova (precum și art. 36 al GDPR). Operatorul trebuie să se consulte cu Centrul anterior prelucrării în cazurile în care evaluarea a impactului asupra protecției datelor, precum se menționează la art. 40, indică că prelucrarea ar genera un risc ridicat dacă controlorul nu întreprinde măsuri pentru a reduce riscul. În așa cazuri art. 41 alin. 2 prevede:

> Atunci când 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 către operator, Centrul oferă consultare în scris operatorului și, după caz, persoanei împuternicite de operator, în cel mult 2 luni de la primirea cererii de consultare, și își poate utiliza oricare dintre competențele menționate de prezenta lege și Legea Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova. Această perioadă poate fi prelungită cu cel mult 2 luni, ținându-se seama de complexitatea prelucrării prevăzute. Centrul informează operatorul și, după caz, persoana împuternicită de operator, în termen de o lună de la primirea cererii, cu privire la orice astfel de prelungire, prezentând motivele întârzierii. Aceste perioade pot fi suspendate până când Centrul a obținut informațiile pe care le-a solicitat în scopul consultării.

În practică aceasta înseamnă că CNPDP începe să revizuiască DPIA (a se vedea mai jos) și comunică controlorului dacă măsurile întreprinse sunt suficiente pentru atenuarea riscului. În caz contrar Centrul emite decizie respectivă.

III. Atribuțiile Operatorului

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

Deoarece în majoritatea cazurilor o DPIA cere eforturi majore, este recomandabil să verificați cu atenție dacă există o necesitate legală pentru acesta: („poate duce la un risc ridicat pentru drepturile și libertățile persoanelor fizice). Conform art. 40, alin. 3 al proiectului de lege (art. 35 al RGPD) o evaluare a impactului asupra protecției datelor trebuie, în special, să fie solicitată în următoarele cazuri:

☐ evaluare sistematică și extinsă a aspectelor personale referitoare la persoane fizice, care are la bază prelucrarea automată, inclusiv profilarea, și pe care se bazează deciziile care produc efecte juridice asupra persoanei fizice sau afectează în mod semnificativ sau similar de semnificativ persoana fizică; ☐ prelucrarea la scară largă a categoriilor speciale de date menționate la articolul 9 alin. (1), ☐ monitorizarea sistematică pe scară largă a unei zone accesibile publicului. ☐ lista tipurilor de operațiuni de prelucrare în conformitate cu Articolul 41 alineatul 4 (a se vedea mai sus I.D)

Întrucât, conform documentului de lucru 248 „Orientările Grupului de lucru „Articolul 29” privind evaluarea impactului asupra protecției datelor)” (a se vedea mai sus II.A.1), aceasta lista nu este una exhaustivă, există o regulă generală: o operațiune de prelucrare care respectă mai puțin de două din următoarele criterii, poate să nu necesite o DPIA:

- Evaluarea sau scoring, inclusiv profilarea și preconizarea, în special din „aspecte privind performanța persoanei vizate la locul de muncă, situația economică, starea de sănătatea, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările” (Considerentele 71 și 91). Astfel de exemple ar putea include o instituție financiară care își monitorizează clienții printr-o bază de date de tip credit sau printr-o bază de date destinată spălării banilor sau combaterea 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 prezice riscurile pentru boală/sănătate sau pentru a crea un profil de comportament sau de marketing bazat pe utilizarea sau navigarea pe site-ul său web.
- Proces 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 (3) a)). Spre exemplu, prelucrarea poate conduce la excluderea sau discriminarea persoanelor. Prelucrarea cu efect redus sau fără efect asupra persoanelor nu corespunde acestui criteriu specific. Mai multe explicații privind aceste noțiuni vor fi oferite prin viitorul Ghid al Grupului de Lucru Articolul 29 privind profilarea.
- Monitorizare sistematică: prelucrare folosită pentru a observa, monitoriza sau controla persoanele vizate, incluzând colectarea de data prin rețele sau „monitorizarea sistematică a unei zone accesibile publicului” (art. 35 (3) c)) 15 . Acest tip de monitorizare reprezintă un criteriu deoarece datele cu caracter personal pot fi colectate în situații în care persoanele vizate pot să nu fie conștiente de 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 prelucrării în spațiul (sau zonele publice) accesibile publicului.

- Date sensibile: acestea includ categorii speciale de date cu caracter personal așa cum sunt definite în art. 9 (spre exemplu informații privind opiniile politice al persoanelor fizice), precum și date cu caracter personal privind condamnările penale sau infracțiuni, Un exemplu ar fi un spital general care păstrează dosarele medicale ale pacienților sau un anchetator privat care păstrează detaliile infractorilor. Dincolo de aceste prevederi ale RGPD, anumite categorii de date pot fi considerate că ar crește riscul posibil pentru drepturile și libertățile persoanelor cum ar fi comunicațiile electronice, datele de localizare, datele financiare care ar pute fi folosite pentru fraudarea plăților). În acest sens, ar putea fi relevant dacă datele au fost deja puse la dispoziția publicului de către persoana vizată sau de terți. Faptul că datele cu caracter personal sunt disponibile în mod public poate fi considerat un factor în evaluarea dacă datele se preconizează a fi utilizate în continuare în anumite scopuri. Acest criteriu poate include, de asemenea, informația prelucrată de o persoană fizică în cursul activităților pur personale sau casnice (cum ar fi servicii de cloud computing pentru gestionarea documentelor personale, e-mailurile, jurnalele, notele de la cititorii electronici echipate cu funcții de notare și informații foarte personale conținute în aplicațiile de log), divulgarea sau prelucrarea cărora în scopuri diferite decât cele casnice ar putea fi percepută ca fiind foarte intruzivă.
- Date prelucrate pe scară largă: RGPD 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 16:
    - numărul persoanelor vizate, ori un număr exact ori un procent din populația relevantă;
    - volumul datelor și/sau gama de elemente diferite de date în curs de prelucrare;
    - durata sau permanența activității de prelucrare a datelor;
    - suprafața geografică a activității de prelucrare
- 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 persoanei vizate.
- Date privind persoanele vizate vulnerabile (Considerentul 75): prelucrarea acestui tip de date este un criteriu din cauza dezechilibrului de putere crescut între persoanele vizate 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. Spre exemplu, angajații ar întâmpina des dificultăți în a se opune prelucrării realizate de către angajator atunci când aceasta este necesar pentru gestionarea resurselor umane, De asemenea, pot fi considerați incapabili să se opună sau să consimtă sau să se opună în mod deliberat la prelucrarea datelor lor. Aceasta include, de asemenea, segmentele mai vulnerabile ale populației cum ar fi (persoane bolnave, solicitanți de azil sau vârstnici, pacienți etc.) și, în orice caz, poate fi identificat un dezechilibru în relația dintre poziția persoanei vizate și operator.
- Utilizare inovatoare sau implementarea unor noi soluții tehnologice sau organizaționale cum ar fi combinarea utilizării amprentei digitale cu recunoașterea facială pentru îmbunătățirea controlului accesului fizic etc. RGPD clarifică (art. 35 (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 utilizarea 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.

- Transferul transfrontalier al datelor în afara Uniunii Europene (considerentul 116), luând în considerare, printre altele, țara sau țările de destinație, posibilitatea transferurilor ulterioare sau probabilitatea transferurilor în baza unor derogări pentru situațiile specifice stabilite de GDPR
- 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). Acestea includ operațiuni de prelucrare care vizează permiterea, modificarea sau refuzarea accesului persoanelor fizice la un serviciu încheierea unui contract. Un exemplu ar putea fi atunci când o bancă își verifică clienții prin compararea cu o bază de date referitoare la credit pentru a decide acordarea unui împrumut.

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)	date sensibile sau date de natură foarte personală. - Date privind persoanele fizice vulnerabile.	NU
Utilizarea unui sistem de camere pentru a monitoriza comportamentul de condus 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 organizaționale.	
O companie monitorizează în mod sistematic activitatea propriilor angajați, inclusiv monitorizarea stațiilor de lucru ale angajaților, activitatea pe Internet etc.	Monitorizare sistematică. - Date privind persoanele vizate vulnerabile.	DA
Colectarea de date de social media publice pentru generarea de profiluri	Evaluare sau scoring. Date prelucrate pe scară largă.	
Un magazine online care utilizează lista e-mailuri pentru a trimite abonaților săi raporturile sale zilnice	Niciuna	
Un site web 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.	

B. Realizarea unei DPIA

Odată ce operatorul constată necesitatea realizării unei DPAI, el poate utiliza instrumentul comprehensiv open source al CNIL (https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment). 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. Mai multe instrumente de vizualizare oferă modalități de a înțelege rapid riscurile. Această aplicație este 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 care trebuie implementat în serverul organizației dvs. Disponibil atât în regim front-end cât și în back-end. Codul este de tip open source și poate fi adaptat la software-ul dvs. Puteți găsi un tutorial video pe https://www.youtube.com/watch?v=-SdA9L4j0a8.

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 controalele selectate de 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 grație unui design care respectă confidențialitatea (confidențialitatea în momentul conceperii (art. 25 GDPR). Ea poate, de asemenea, fi utilizată de CNPDP pentru revizuirea DPIA în cazul consultărilor prealabile (a se vedea mai sus II.B).

Mai mult, puteți beneficia și de o bază cuprinzătoare de cunoștințe pe https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf. În ceea ce privește măsurile adecvate, spre deosebire de Modelul German Standard de Protecție a Datelor care este întemeiat pe scopuri speciale de protecție (dar fără un instrument software și versiuni non-germane deocamdată), acest instrument se concentrează asupra amenințărilor, riscurilor și măsuri adecvate în dependență de nivelul de severitate și probabilitate (a se vedea mai jos III.B.4).

În orice caz, documentul de lucru 248 al Grupului de Lucru Articolul 29 Orientări Privind evaluarea impactului asupra protecției datelor" (a se vedea mai sus II.A.1) identifică în Anexa 2 criteriile comune pe care trebuie să le îndeplinească o DPIA efectuată pentru a răspunde cerințelor legale. Aceste criterii sunt următoarele:

1. Descrierea sistematică a operațiunilor de prelucrare prevăzute și scopul prelucrării, inclusiv, dacă este cazul, interesul legitim urmărit de operator (alineatul 3, lit. a)

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 II.A.1), DPIA trebuie să respecte următoarele criterii:

□ natura, sfera, contextul și scopurile prelucrării sunt luate în considerare (considerentul 90); De ex. camere de supraveghere la intrarea într-o sală de sport pentru prevenirea furtului

 sunt înregistrate datele personale, destinatarii și perioada pentru care vor fi stocate datele cu caracter personal;
De ex. datele angajaților și clienților din camerele de supraveghere vor fi stocate timp de 30 de zile
 este furnizată o descriere funcțională a operațiunii de prelucrare;
De ex. datele din camerele de supraveghere vor fi utilizate în cazul infracțiunilor
 sunt identificate activele pe care se bazează datele personale (hardware, software, rețele, persoane, canale de transmisie pe hârtie sau pe hârtie);
De ex. camerele, software de video management folosite
 se ține cont de respectarea codurilor de conduită aprobate (Articolul 35 alineatul (8) GDPR)

2. Evaluarea necesității și proporționalității operațiunilor de prelucrare în raport cu scopurile (alineatul 3, lit. b)

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 II.A.1), DPIA trebuie să respecte următoarele criterii:

măsurile preconizate pentru conformarea cu Regulamentului sunt determinate [Articolul 35 alineatul (7) litera (d) GDPR și considerentul 90], ținând cont de:
 măsurile care contribuie la proporționalitatea și necesitatea prelucrării în baza:
 scopului (urilor) specificate, explicite și legitime (Articolul 5 alineatul (1) litera (b) GDPR);
De ex. pentru prevenirea furturilor
 legalitatea prelucrării (Articolul 6 GDPR);
De ex. interesul legitim (ar putea, de ademenea fi un contract pentru clienți), Art. 93 al proiectului de lege
 adecvate, relevante și limitate la datele necesare [Articolul 5 alineatul (1) litera (c)];
De ex. limitat la zona de intrare, alte zone nu se supraveghează
 durată de stocare limitată (Articolul 5 alineatul (1) litera (e));
De ex. 30 de zile
 măsurile care contribuie la drepturile subiecților de date:
 informații furnizate subiectului de date (Articolele 12, 13 și 14);
De ex. informație pe site, panou de informații
 dreptul de acces și portabilitatea datelor (articolele 15 și 20);
De ex. asigurarea unui formular
 dreptul la rectificare și dreptului la ștergere (Articolele 16, 17 și 19);
De ex. asigurarea unui formular
 dreptul la obiecție și la limitarea prelucrării (Articolele 18, 19 și 21);
De ex. asigurarea unui formular
 relațiile cu persoanele împuternicite de operator (articolul 28 GDPR);
De ex. verificarea contractelor cu companiile de instalare și menținere
 garanțiile privind transferul (transferurile) internațional (capitolul V);
De ex. date din cloud
 consultația prealabilă (Articolul 36 GDPR).

3. Evaluarea riscurilor la adresa drepturilor și libertăților subiecților de date (alineatul 3, lit. c)

Scopul acestei prevederi este de a înțelege bine controalele 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 II.A.1), o DPIA trebuie să respecte următoarele criterii:

□ originea, natura, particularitatea și gravitatea riscurilor sunt estimate (a se vedea considerentul 84) sau, mai exact, pentru fiecare risc de ex. acces nelegitim, modificări nedorite și dispariția datelor)
□ sursele de risc sunt luate în considerare (considerentul 90); de ex. uși neîncuiate, acces nerestricționat la baza de date □ impactele potențiale asupra drepturilor și libertăților subiecților de date sunt identificate în cazul unor evenimente care includ accesul nelegitim, modificări nedorite și dispariția datelor; de ex. publicarea imaginilor video din sala de sport a unei persoane aflate pe foaie de boală care este ☐ amenințări care ar putea duce la acces nelegitim, identificarea modificărilor nedorite și dispariția datelor; ☐ de ex. accesul angajaților probabilitatea și severitatea sunt estimate (considerentul 90); Conform instrumentului DPIA CNIL acest criteriu poate fi neglijabil limitat, semnificativ sau Maxim. Pentru detalii a se vedea pagina 5 a bazei de cunoștințe 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 și ale altor persoane în cauză (alineatul 3, lit. d)

Articolele 5, 12, 25 și 32 prevăd cerințe esențiale privind securitatea prelucrării datelor cu caracter personal. Regulamentul solicită măsuri tehnice și organizatorice adecvate pentru a garanta un nivel de protecție adecvat riscului (Articolul 32 alineatul (1)). În plus, GDPR impune o procedură de revizuire periodică, analiză și evaluare a eficacității măsurilor tehnice și organizatorice [Articolul 32 alineatul (1) litera (d)]. GDPR oferă posibilitatea evaluării procedurilor bazate pe IT în codurile de conduită și prin mecanisme de certificare (Articolele 40-43 GDPR).

Articolul 5 GDPR 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.

Aici, de asemenea, poate fi consultată baza de cunoștințe a instrumentului DPIA francez pe https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf. Eu recomand combinarea acestuie cu abordarea mai detaliată și măsurile structurizate ale Modelul Standard de Protecție a Datelor (SDM). În noiembrie 2016, Conferința autorităților independente de protecție a datelor a Federației și Landurilor a autorizat SDM pentru publicare. Chiar dacă acesta a fost intenționată să armonizeze diferitele cerințe ale diferitelor legi ale Landur-ilor privind protecția datelor, aceasta este pe deplin conformă cu GDPR.

Modelul standard de protecție a datelor (SDM) oferă mecanisme adecvate pentru a transfera acerințele legale ale GDPR în măsuri tehnice și organizatorice. Pentru a atinge acest scop, SDM structurează cerințele legale în ceea ce privește cele șapte 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) al GDPR, precum și în Articolul 25. Datele cu caracter personal sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile pentru care sunt prelucrate.

Scopul de protecție prin minimizarea datelor poate fi realizat prin:

- Reducerea atributelor colectate ale subiectului de date, (de ex. nu se colectează datele de naștere dacă nu este necesar)
- Reducerea opțiunilor de prelucrare în operațiuni de prelucrare, (de ex. lista definitivă a destinatarilor)
- Reducerea posibilităților de cunoaștere a datelor existente, (de ex. acces limitat)
- Preferința pentru operațiunile de prelucrare automată (nu pentru procesele de luare a deciziilor), care fac inutilă utilizarea datelor prelucrate și limitează posibilitatea unor interferențe, comparative cu procesele de dialog controlate, (recuperarea automată a unui set limitat de informații dintr-o bază de date dacă condițiile sunt îndeplinite clar definite)
- Implementarea metodelor de rutină automate de blocare și ștergere; procedurile de pseudonimizare și anonimizare, (de ex. a se vedea art. 35 al proiectului de lege)
- Reguli pentru a controla procesele pentru schimbarea procedurilor (de ex. competențele definite)

b) Disponibilitatea

Principiul disponibilității este explicit inclus în Articolul 32 alineatul (1) literele (b) și (c) în contextul securității procesării datelor. El este, de asemenea, ancorat în Articolul 5 alineatul (1) litera (e) din GDPR 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 (Articolele 13 și 15 din GDPR). Disponibilitatea obiectivului de protecție este, de asemenea, o condiție esențială pentru dreptul la portabilitatea datelor (articolul 20 GDPR).

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 sintaxei de date,
- 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 Articolul 5 alineatul (1) litera (f) al GDPR, precum și în Articolul 32 al GDPR. 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 sumelor de control, sigiliilor electronice și a semnăturilor în prelucrarea datelor în conformitate cu un concept criptografic,
- Atribuirea documentată a drepturilor și a rolurilor,
- Procesele 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 regulată a detectabilității determinării respective a stării actuale a proceselor.

d) Confidențialitatea

Obligația de a păstra confidențialitatea rezultă în special din Articolul 5 alineatul (1) litera (f) din GDPR, din Articolul 32 alineatul (1) litera (b) din GDPR și din Articolul 38 alineatul 5 din GDPR (obligația de confidențialitate a responsabilului cu protecția datelor) (3) (b) GDPR (obligația de confidențialitate a

persoanei împuternicite de operatorul de date). Acesta asigură protecția împotriva prelucrării neautorizate și ilegale. O încălcare a confidențialității în general constituie o prelucrare a datelor fără o bază legală.

Măsurile tipice de garantare a confidențialității sunt:

• Definirea conceptului de drepturi și rol 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 specificate (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 se găsește în special în baza juridică individuală de prelucrare (Art. 6 GDPR) care face ca obiectivele ce țin de afaceri, scopurile cercetării etc. să fie un criteriu. Acestea sunt incluse în Regulamentul General privind Protecția Datelor prin intermediul principiului limitării scopului de la Articolul 5 alineatul (1) litera (b). În cazul prelucrării datelor pe bază de consimțământ, din Articolul 7 alineatul (4) din GDPR rezultă că consimțământul poate fi nevalabil dacă datele nu sunt necesare pentru îndeplinirea scopului. O măsură tipică pentru necorelare este, de exemplu, pseudonimizarea menționată la Articolul 40 alineatul (2) litera (d) din GDPR.

Măsurile tipice de garantare a necorelării sunt:

• Restricționarea drepturilor de procesare, utilizare și transfer, • În ceea ce privește programarea, omiterea sau închiderea interfețelor în procedurile și componentele procedurilor, • Dispoziții de reglementare pentru interzicerea backdoors, 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 pseudonime sau anonime, • Proceduri reglementate pentru modificarea scopului.

f) Transparența

Principiul transparenței este prevăzut la Articolul 5 alineatul (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 afaceri, 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 sau 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 (Logging) accesului și a modificărilor,
• Verificarea surselor de date (autenticitate),
• Versiunea de control,
• Documentarea procedurilor de prelucrare prin intermediul protocoalelor pe baza unui certificat conceptul de logging și evaluare,
• Examinarea drepturilor subiectului de date vizat în conceptul de logging și evaluare.

g) Dreptul de intervenție (Intervenability)

Dreptul de intervenție al subiectului de date vizat este în mod explicit derivat din dispozițiile privind rectificarea, blocarea, ștergerea și dreptul de opoziție (Articolele 16-17 din GDPR). Acestea pot rezulta, de asemenea, dintr-o ponderare a intereselor în cadrul unor criterii legale de prelucrare legală. Încă o dată, operatorul trebuie să furnizeze, în conformitate cu Articolul 5 alineatul (1) litera (d), condiția prealabilă pentru garantarea acestor drepturi, atât la nivel organizațional, cât și, dacă este necesar, la nivel tehnic.

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, în mod consistent corect, 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. Diferit față de standardele de securitate a informațiilor care se concentrează pe protejarea organizației de prelucrare 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 protecție a securității informațiilor, este obișnuit metodologic să se măsoare cantitatea de daune și probabilitatea de apariție și să se evalueze riscul care rezultă din acestea. Cu toate acestea, protecția (drepturilor fundamentale) a 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.

<u>Nivelul de protecție categoria ‘normal’</u>

Întrucât orice prelucrare a datelor cu caracter personal reprezintă o ingerință în drepturile fundamentale ale persoanei vizate, 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.

<u>Nivelul de protecție categoria ‘ridicat’</u>

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 neambiguu, date cu nivel ridicat de interconexiune (de exemplu, numărul de asigurare de sănătate valabil pe toată durata de viață a persoanei vizate, codul fiscal);
• Lipsa de transparență legală sau care urmează a fi justificată pentru subiectele de date în ceea ce privește procedurile (de exemplu, protecția de stat, valorile estimate în punctaj);
• 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 în bandă mare și largă)
• Riscul de discriminare, stigmatizare (de exemplu, prin intermediul algoritmilor, realizarea netransparentă a deciziilor referitoare la subiectul de date);
• Intervenția în domeniile protejate în mod special ale vieții unui subiect de date.

Nivelul de protecție categoria 'foarte ridicat'

Un nivel 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 I.D.1), DPIA trebuie să respecte următoarele criterii:

☐ se solicită avizul Responsabilului de Protecție a Datelor (DPO) (Articolul 35 alineatul (2));
☐ sunt solicitate opiniile subiecților de date sau ale reprezentanților acestora (Articolul 35 alineatul (9)).

Dacă este cazul, operatorul ar trebui să intre în contact cu părțile interesate precum și, de ex., cu sindicate, a se vedea art. 93.d) al proiectului de lege.

IV. Rezumatul

Eu recomand ca CNPDP să înceapă cât mai curând posibil să elaboreze o listă alb negru menționată în art. 40, alin. 4, 5 al proiectului de lege. Centrul poate beneficia de documentele existente ale Autorităților de Protecție a Datelor din statele membre. Deoarece în majoritatea cazurilor realizarea unei DPIA necesită depunerea unui efort major, se recomandă de a lansa un proces în care ar fi implicate toate părțile interesate. Mai mult, personalul CNPDP însuși ar trebui să se familiarizeze cu instrumentul DPIA francez al CNIL, întrucât aceasta ar facilita consultarea prealabilă în cazurile în care se aplică art. 41. Instrumentul este disponibil în limba română.

După ce CNPDP se familiarizează cu instrumentul, el ar trebui să comunice necesitatea realizării unei DPIA **operatorilor** care prelucrează date stipulate în art. 40, susceptibile să genereze „riscuri ridicate pentru drepturile și libertățile persoanelor fizice", (operatori precum spitale, agenții de rating etc.). Întrucât instrumentul DPIA francez al CNIL este destinat pentru utilizarea de către operatori, el trebuie promovat în mod corespunzător. Operatorii trebuie de pe acum să realizeze o verificare internă a legalității (în special în ceea ce privește necesitatea) și documentația operațiunilor de prelucrare a datelor cu caracter personal.