GRUPUL DE LUCRU PENTRU PROTECȚIA DATELOR INSTITUIT ÎN TEMEIUL ARTICOLULUI 29

17/RO

WP 248 rev. 01

Orientări privind evaluarea impactului asupra protecției datelor (DPIA) și modul în care se determină dacă prelucrarea este „susceptibilă să genereze un risc ridicat” în sensul Regulamentului 2016/679

Adoptate la 4 aprilie 2017

Revizuite și adoptate la 4 octombrie 2017

GRUPUL DE LUCRU PENTRU PROTECȚIA PERSOANELOR ÎN CEEA CE PRIVEȘTE PRELUCRAREA DATELOR CU CARACTER PERSONAL

instituit prin Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995,

având în vedere articolele 29 și 30 din directivă,

având în vedere regulamentul său de procedură,

ADOPTĂ PREZENTELE ORIENTĂRI:

Cuprins

I. Introducere

Regulamentul 2016/679[1] (Regulamentul general privind protecția datelor, GDPR) se va aplica de la 25 mai 2018. Articolul 35 din GDPR introduce conceptul de evaluare a impactului asupra protecției datelor (DPIA[2]), la fel ca Directiva 2016/680[3].

DPIA este un proces conceput pentru a descrie prelucrarea, a evalua necesitățile și proporționalitățile acesteia și a contribui la gestionarea riscurilor la adresa drepturilor și libertăților persoanelor fizice care rezultă din prelucrarea datelor cu caracter personal[4], prin evaluarea acestora și stabilirea de măsuri pentru soluționarea lor. DPIA sunt instrumente importante pentru asumarea răspunderii, întrucât acestea ajută operatorii să respecte cerințele GDPR, dar și să demonstreze că au fost luate măsurile corespunzătoare în vederea asigurării conformității cu regulamentul (a se vedea, de asemenea, articolul 24)[5]. Cu alte cuvinte, **o DPIA este un proces de consolidare și demonstrare a conformității**.

Conform GDPR, neconformitatea cu cerințele DPIA poate conduce la aplicarea de amenzi de către autoritatea de supraveghere competentă. Neefectuarea unei DPIA atunci când prelucrarea face obiectul unei DPIA [articolul 35 alineatul (1) și alineatele (3)-(4)], efectuarea unei DPIA într-un mod incorect

---

[1] 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).

[2] Termenul „evaluarea impactului asupra vieții private" (PIA) este adesea utilizat în alte contexte pentru a se face referire la aceeași noțiune.

[3] Articolul 27 din Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date prevede, de asemenea, că o evaluare a impactului asupra vieții private este necesară atunci când „*[prelucrarea este susceptibilă] să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice*".

[4] GDPR nu definește în mod oficial noțiunea de DPIA ca atare, însă

- conținutul minim al acesteia este precizat la articolul 35 alineatul (7), după cum urmează:
  - „*(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".*
- semnificația și rolul acesteia sunt clarificate în considerentul 84 după cum urmează: „*Pentru a favoriza respectarea dispozițiilor prezentului regulament în cazurile în care operațiunile de prelucrare sunt susceptibile să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul ar trebui să fie responsabil de efectuarea unei evaluări a impactului asupra protecției datelor, care să estimeze, în special, originea, natura, specificitatea și gravitatea acestui risc".*

[5] A se vedea, de asemenea, considerentul 84: „*Rezultatul evaluării ar trebui luat în considerare la stabilirea măsurilor adecvate care trebuie luate pentru a demonstra că prelucrarea datelor cu caracter personal respectă prezentul regulament*".

[articolul 35 alineatul (2) și alineatele (7)-(9)] sau neconsultarea autorității de supraveghere competente atunci când este necesar [articolul 36 alineatul (3) litera (e)] poate conduce la aplicarea unei amenzi administrative de până la 10 milioane EUR sau, în cazul unei întreprinderi, de până la 2 % din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare.

II. Domeniul de aplicare a orientărilor

Prezentele orientări iau în considerare:

- declarația 14/EN WP 218 a Grupului de lucru pentru protecția datelor instituit în temeiul articolului 29 (WP29)[6];
- ghidul WP29 privind responsabilul cu protecția datelor 16/EN WP 243[7];
- avizul WP29 privind limitarea scopului 13/EN WP 203[8];
- standardele internaționale[9].

În conformitate cu abordarea bazată pe riscuri prevăzută de GDPR, efectuarea unei DPIA nu este obligatorie pentru fiecare operațiune de prelucrare. O DPIA este necesară numai atunci când prelucrarea este „*susceptibil[ă] să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice*” [articolul 35 alineatul (1)]. Pentru a asigura o interpretare coerentă a împrejurărilor în care o DPIA este obligatorie [articolul 35 alineatul (3)], prezentele orientări vizează în primul rând clarificarea acestei noțiuni și furnizarea de criterii pentru listele care urmează să fie adoptate de către autoritățile pentru protecția datelor (APD) în temeiul articolului 35 alineatul (4).

În conformitate cu articolul 70 alineatul (1) litera (e), Comitetul european pentru protecția datelor (EDPB) va fi în măsură să emită orientări, recomandări și cele mai bune practici pentru a încuraja aplicarea coerentă a GDPR. Scopul prezentului document este de a anticipa astfel de activități viitoare ale EDPB și, prin urmare, de a clarifica dispozițiile relevante din GDPR pentru a ajuta operatorii să respecte legea și a furniza certitudine juridică operatorilor care trebuie să efectueze o DPIA.

Prezentele orientări urmăresc, de asemenea, să încurajeze elaborarea:

- unei liste comune la nivelul Uniunii Europene de operațiuni de prelucrare pentru care o DPIA este obligatorie [articolul 35 alineatul (4)];
- unei liste comune la nivelul UE de operațiuni de prelucrare pentru care nu este necesară o DPIA [articolul 35 alineatul (5)];
- unor criterii comune privind metodologia de realizare a unei DPIA [articolul 35 alineatul (5)];

---

[6] Declarația 14/EN WP 218 a WP29 privind rolul unei abordări bazate pe riscuri a cadrelor juridice privind protecția datelor, adoptată la 30 mai 2014.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

[7] Ghidul WP29 privind responsabilul cu protecția datelor 16/EN WP 243, adoptat la 13 decembrie 2016;
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[8] Avizul 03/2013 al WP29 privind limitarea scopului 13/EN WP 203, adoptat la 2 aprilie 013.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[9] de exemplu, ISO 31000: 2009 Gestionarea riscurilor — *Principii și orientări*, Organizația Internațională de Standardizare (ISO); ISO/IEC 29134 (project), *Tehnologia informației — Tehnici de securitate —Evaluarea impactului asupra vieții private* — Orientări, Organizația Internațională de Standardizare (ISO).

- unor criterii comune pentru precizarea cazurilor în care se consultă autoritatea de supraveghere [articolul 36 alineatul (1)];
- unor recomandări bazate, dacă este posibil, pe experiența acumulată în statele membre ale UE.

III. DPIA: regulamentul explicat

GDPR impune operatorilor să pună în aplicare măsuri adecvate pentru a garanta și pentru a putea demonstra conformitatea cu GDPR, ținând seama, printre altele, de „riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice” [articolul 24 alineatul (1)]. Obligația operatorilor de a efectua o DPIA în anumite situații ar trebui să fie înțeleasă în contextul obligației lor generale de a gestiona în mod corespunzător riscurile[10] prezentate de prelucrarea datelor cu caracter personal.

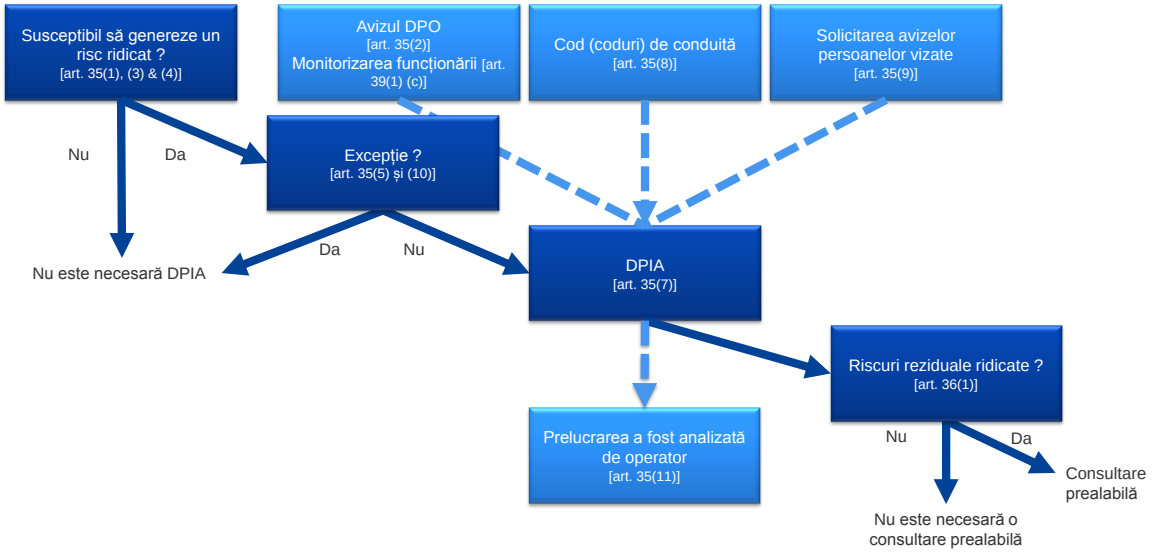
Un „risc” este un scenariu care descrie un eveniment și consecințele acestuia, estimate în ceea ce privește gravitatea și probabilitatea. Astfel, „gestionarea riscului” poate fi definită ca activitățile coordonate pentru conducerea și controlul unei organizații în ceea ce privește riscurile.

Articolul 35 se referă la un posibil risc ridicat „pentru drepturile și libertățile persoanelor”. Astfel cum este indicat în declarația grupului de lucru pentru protecția datelor instituit în temeiul articolului 29 cu privire la o abordare bazată pe riscuri a cadrelor juridice privind protecția datelor, trimiterea la „drepturile și libertățile” persoanelor vizate se referă în primul rând la dreptul la protecția datelor și a vieții private, dar poate include, de asemenea, alte drepturi fundamentale, cum ar fi libertatea de exprimare, libertatea de gândire, libertatea de circulație, interzicerea discriminării, dreptul la libertate, conștiință și religie.

În conformitate cu abordarea bazată pe risc prevăzută de GDPR, efectuarea unei DPIA nu este obligatorie pentru fiecare operațiune de prelucrare. În schimb, o DPIA este necesară numai în cazul în care un tip de prelucrare este „susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice” [articolul 35 alineatul (1)]. Simplul fapt că respectivele condiții care declanșează obligația de a efectua DPIA nu au fost îndeplinite nu diminuează, cu toate acestea, obligația generală a operatorilor de a pune în aplicare măsuri pentru a gestiona în mod corespunzător riscurile la adresa drepturilor și libertăților persoanelor vizate. În practică, acest lucru înseamnă că operatorii trebuie să evalueze în permanență riscurile generate de activitățile lor de prelucrare pentru a identifica acele cazuri în care un tip de prelucrare este „susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice”.

[10] Trebuie subliniat faptul că, pentru a gestiona riscurile pentru drepturile și libertățile persoanelor fizice, riscurile trebuie să fie identificate, analizate, estimate, evaluate, tratate (de exemplu, atenuate...) și revizuite în mod regulat. Operatorii nu pot evita răspunderea lor prin acoperirea riscurilor în cadrul polițelor de asigurare.

Figura de mai jos ilustrează principiile de bază legate de DPIA din GDPR:



A. Ce abordează o DPIA? O singură operațiune de prelucrare sau un set de operațiuni de prelucrare similare?

O DPIA ar putea să vizeze o singură operațiune de prelucrare a datelor. Cu toate acestea, articolul 35 alineatul (1) prevede că „*o evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare*". Considerentul 92 adaugă că „*în unele circumstanțe ar putea fi rezonabil și util din punct de vedere economic ca o evaluare a impactului asupra protecției datelor să aibă o perspectivă mai extinsă decât cea a unui singur proiect, de exemplu în cazul în care autorități sau organisme publice intenționează să instituie o aplicație sau o platformă de prelucrare comună sau în cazul în care mai mulți operatori preconizează să introducă o aplicație comună sau un mediu de prelucrare comun în cadrul unui sector sau segment industrial sau pentru o activitate orizontală utilizată la scară largă*".

Ar putea fi utilizată o singură DPIA pentru a evalua mai multe operațiuni de prelucrare similare în ceea ce privește natura, domeniul de aplicare, contextul, scopul și riscurile. Într-adevăr, evaluările DPIA urmăresc în mod sistematic studierea unor situații noi care ar putea conduce la riscuri ridicate pentru drepturile și libertățile persoanelor fizice și nu este necesar să se efectueze o DPIA în cazurile (și anume, operațiunile de prelucrare efectuate într-un context specific și pentru un anumit scop) care au fost deja studiate. Acest lucru ar putea fi valabil în cazul în care o tehnologie similară este utilizată pentru colectarea aceluiași tip de date pentru aceleași scopuri. De exemplu, un grup de autorități municipale care instituie fiecare un sistem CCTV similar ar putea să efectueze o singură DPIA care acoperă prelucrarea de către respectivii operatori diferiți, sau un operator feroviar (operator unic) ar putea acoperi supravegherea video în toate stațiile sale de tren printr-o singură DPIA. Acest lucru poate fi aplicabil, de asemenea, diferitelor operațiuni de prelucrare similare puse în aplicare de diverși operatorii de date. În aceste cazuri, ar trebui să fie partajată sau pusă la dispoziția publicului o trimitere la DPIA, măsurile descrise în DPIA trebuie să fie puse în aplicare și trebuie furnizată o justificare pentru efectuarea unei DPIA unice.

Atunci când operațiunea de prelucrare implică operatori asociați, aceștia trebuie să definească obligațiile lor respective în mod exact. DPIA a acestora ar trebui să stabilească partea care este

responsabilă pentru diferitele măsuri concepute pentru a trata riscurile și pentru a proteja drepturile și libertățile fundamentale ale persoanelor vizate. Fiecare operator de date ar trebui să își exprime necesitățile și să facă schimb de informații utile fără a compromite secretele (de exemplu, protecția secretelor comerciale, proprietatea intelectuală, informații comerciale confidențiale) sau fără a dezvălui vulnerabilitățile.

O DPIA poate fi utilă, de asemenea, pentru a evalua impactul unui produs al tehnologiei asupra protecției datelor, de exemplu, al unui element de hardware sau software, atunci când este posibil ca acesta să fie utilizat de diferiți operatori de date pentru a efectua diferite operațiuni de prelucrare. Desigur, operatorul de date care utilizează produsul este în continuare obligat să efectueze propria DPIA în ceea ce privește punerea în aplicare specifică, dar aceasta se poate baza pe o DPIA elaborată de furnizorul produsului, dacă este cazul. Un exemplu ar putea fi relația dintre producătorii de contoare inteligente și companiile de utilități. Fiecare furnizor de produse sau persoană împuternicită de operator ar trebui să facă schimb de informații utile, fără a compromite secrete și fără a genera riscuri de securitate prin divulgarea vulnerabilităților.

B. Care sunt operațiunile de prelucrare care fac obiectul unei DPIA? În afară de excepții, operațiunile de prelucrare „*susceptibile să genereze un risc ridicat*”.

Prezenta secțiune descrie cazurile în care DPIA este obligatorie și cazurile în care nu este necesară efectuarea unei DPIA.

În afară de cazul în care operațiunea de prelucrare constituie o excepție (III.B.a), DPIA trebuie efectuată dacă o operațiune de prelucrare este „*susceptibil[ă] să genereze un risc ridicat*” (III.B.b).

a) Când este o DPIA obligatorie? Atunci când prelucrarea este „*susceptibil[ă] să genereze un risc ridicat*”.

GDPR nu solicita efectuarea unei DPIA pentru fiecare operațiune de prelucrare care poate genera riscuri pentru drepturile și libertățile persoanelor fizice. Efectuarea unei DPIA este obligatorie numai în cazul în care prelucrarea este „*susceptibil[ă] să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice*” [articolul 35 alineatul (1), ilustrat de articolul 35 alineatul (3) și completat de articolul 35 alineatul (4)]. Aceasta este deosebit de importantă atunci când se introduce o nouă tehnologie de prelucrare a datelor[11].

În cazurile în care nu este clar dacă este necesară o DPIA, WP29 recomandă efectuarea, cu toate acestea, a unei DPIA, întrucât o DPIA este un instrument util pentru a sprijini operatorii să respecte legislația în materie de protecție a datelor.

Cu toate că o DPIA ar putea fi solicitată și în alte împrejurări, articolul 35 alineatul (3) prevede o serie de exemple atunci când o operațiune de prelucrare este „*susceptibil[ă] să genereze riscuri ridicate*”:

- „(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*

[11] A se vedea considerentele 89, 91 și articolul 35 alineatele (1) și (3) pentru exemple suplimentare.

baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă"[12]**;**

- *(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*[13]*; sau*
- *(c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului*".

Astfel cum indică formularea „*mai ales*" din teza introductivă a articolului 35 alineatul (3) din GDPR, aceasta este o listă neexhaustivă. Pot exista operațiuni de prelucrare cu „*risc ridicat*" care nu sunt incluse în această listă, dar care prezintă totuși riscuri ridicate similare. Aceste operațiuni de prelucrare, de asemenea, ar trebui să fie supuse unor DPIA. Din acest motiv, criteriile dezvoltate mai jos depășesc uneori o simplă explicație a ceea ce ar trebui să se înțeleagă prin cele trei exemple prezentate în articolul 35 alineatul (3) din GDPR.

Pentru a furniza un set mai concret de operațiuni de prelucrare care necesită o DPIA din cauza riscului lor ridicat inerent, luând în considerare elementele specifice ale articolului 35 alineatele (1) și (3) literele (a)-(c), lista care urmează să fie adoptată la nivel național în temeiul articolului 35 alineatul (4) și al considerentelor 71, 75 și 91, precum și al altor trimiteri din GDPR la operațiuni de prelucrare „*susceptibile să genereze un risc ridicat*"[14], ar trebui să fie luate în considerare următoarele nouă criterii.

1. Evaluarea sau punctarea, inclusiv crearea de profiluri și preconizarea, în special de la *„aspecte privind randamentul la locul de muncă al persoanei vizate, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările*" (considerentele 71 și 91). Exemple în acest sens ar putea include o instituție financiară care își monitorizează clienții într-o bază de date de credit de referință sau într-o bază de date pentru combaterea spălării banilor sau pentru combaterea finanțării terorismului (AMP/CTF) sau o bază de date privind frauda, sau o întreprindere de biotehnologie care oferă teste genetice în mod direct consumatorilor pentru a evalua și a preconiza boala/riscurile pentru sănătate, sau o societate care creează profiluri comportamentale sau de comercializare pe baza utilizării sau a navigației pe site-ul său.
2. Luarea de decizii în mod automat cu un efect juridic sau similar semnificativ: prelucrarea care are ca scop luarea deciziilor privind persoanele vizate care produc „*efecte juridice privind persoana fizică*" sau care „*o afectează în mod similar într-o măsură semnificativă*" [articolul 35 alineatul (3) litera (a)]. De exemplu, prelucrarea poate conduce la excluderea sau discriminarea persoanelor. Prelucrarea cu efect limitat sau inexistent asupra persoanelor nu corespunde acestui criteriu specific. Explicații suplimentare privind aceste noțiuni vor fi furnizate în cadrul viitoarelor orientări ale WP29 privind crearea de profiluri.

---

[12] A se vedea considerentul 71: „*în special analizarea sau previzionarea unor aspecte privind randamentul la locul de muncă, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările, în scopul de a se crea sau de a se utiliza profiluri personale*".

[13] A se vedea considerentul 75: „*datele cu caracter personal prelucrate sunt date care dezvăluie originea rasială sau etnică, opiniile politice, religia sau convingerile filozofice, apartenența sindicală; sunt prelucrate date genetice, date privind sănătatea sau date privind viața sexuală sau privind condamnările penale și infracțiunile sau măsurile de securitate conexe*";

[14] A se vedea, de exemplu, considerentele 75, 76, 92, 116.

3. Monitorizarea sistematică: prelucrarea utilizată pentru observarea, monitorizarea sau controlul persoanelor vizate, inclusiv datele colectate prin intermediul rețelelor sau al „ *unei monitorizări sistematice pe scară largă a unei zone accesibile publicului*” [articolul 35 alineatul (3) litera (c)][15]. Acest tip de monitorizare reprezintă un criteriu deoarece datele cu caracter personal pot fi colectate în circumstanțe în care persoanele vizate ar putea să nu știe cine colectează datele lor cu caracter personal și modul în care acestea vor fi utilizate. În plus, ar putea fi imposibil pentru persoanele fizice să evite a fi supuse unei astfel de prelucrări într-un spațiu sau în spații publice (sau accesibile publicului)
4. Date sensibile sau date foarte personale: acestea includ categorii speciale de date cu caracter personal, astfel cum sunt definite la articolul 9 (de exemplu, informații cu privire la opiniile politice ale persoanelor), precum și date cu caracter personal referitoare la condamnări penale sau infracțiuni, astfel cum sunt definite la articolul 10. Un exemplu ar fi un spital general care păstrează dosarele medicale ale pacienților sau un detectiv particular 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 deoarece 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 documente personale, e-mailuri, jurnale, note din dispozitivele electronice de citit echipate cu caracteristici de luare de notițe, precum și informații foarte personale conținute în aplicații de înregistrare a vieții.
5. Datele prelucrate pe scară largă: GDPR nu definește ceea ce constituie pe scară largă, cu toate că în considerentul 91 se oferă unele orientări în acest sens. În orice caz, WP29 recomandă ca în special următorii factori să fie luați în considerare atunci când se stabilește dacă prelucrarea se efectuează pe scară largă[16]:
    a. numărul de persoane vizate în cauză, fie ca număr specific sau ca proporție din populația relevantă;
    b. volumul de date și/sau gama de diferite elemente de date care sunt prelucrate;
    c. durata sau persistența activității de prelucrare a datelor;

[15] WP29 interpretează termenul „*sistematice*” ca însemnând unul sau mai multe dintre următoarele (a se vedea Orientările WP 29 privind responsabilul cu protecția datelor 16/EN WP 243):
- care se produc în conformitate cu un sistem;
- prestabilite, organizate sau metodice;
- care se desfășoară ca parte a unui plan general de colectare a datelor;
- efectuate ca parte a unei strategii.

WP29 interpretează sintagma „*zone accesibile publicului*” ca fiind orice loc deschis pentru orice membru al publicului, de exemplu o piațetă, un centru comercial, o stradă, o piață, o gară sau o bibliotecă publică.

[16] A se vedea Orientările WP29 privind responsabilul cu protecția datelor 16/EN WP 243.

d. extinderea geografică a activității de prelucrare.

6. Corelarea sau combinarea seturilor de date, de exemplu care provin din două sau mai multe operațiuni de prelucrare a datelor efectuate în scopuri diferite și/sau de către diferiți operatori de date într-un mod care ar depăși așteptările rezonabile ale persoanei vizate[17].
7. Date privind persoanele vizate vulnerabile (considerentul 75): prelucrarea acestui tip de date reprezintă un criteriu din cauza dezechilibrului de putere crescut dintre persoanele vizate și operatorul de date, ceea ce înseamnă că persoanele pot să nu fie în măsură a-și da consimțământul sau a respinge cu ușurință prelucrarea datelor lor sau a-și exercita drepturile. Persoanele vizate vulnerabile pot include copii (aceștia pot fi considerați ca nefiind în măsură să se opună sau să își dea consimțământul în mod deliberat și precaut pentru prelucrarea datelor lor), angajați, segmente mai vulnerabile ale populației care necesită o protecție specială (persoane bolnave mintal, solicitanții de azil sau persoanele în vârstă, pacienți etc.) și, în orice caz, atunci când poate fi identificat un dezechilibru între poziția persoanei vizate și cea a operatorului.
8. Utilizarea inovatoare sau aplicarea unor soluții tehnologice sau organizaționale noi, cum ar fi combinarea utilizării amprentei digitale și recunoașterea facială pentru îmbunătățirea controlului accesului fizic etc. GDPR precizează în mod clar [articolul 35 alineatul (1) și considerentele 89 și 91] că utilizarea unei tehnologii noi, definită „*în conformitate cu nivelul atins al cunoștințelor tehnologice*” (considerentul 91), poate declanșa necesitatea realizării unei DPIA. Aceasta se datorează faptului că utilizarea unor astfel de tehnologii poate implica forme noi de colectare și de utilizare a datelor, eventual cu un risc ridicat pentru drepturile și libertățile persoanelor. Într-adevăr, consecințele personale și sociale ale desfășurării unei noi tehnologii pot fi necunoscute. O DPIA va sprijini operatorul de date să înțeleagă și să trateze astfel de riscuri. De exemplu, anumite aplicații de tipul „internetul obiectelor” ar putea avea un impact semnificativ asupra vieții de zi cu zi și a vieții private a persoanelor; prin urmare, acestea necesită o DPIA.
9. Atunci când prelucrarea în sine „*împiedică persoanele vizate să exercite un drept sau să utilizeze un serviciu ori un contract*” (articolul 22 și considerentul 91). Acest lucru include operațiunile de prelucrare care au ca obiectiv permiterea, modificarea sau refuzul accesului persoanelor vizate la un serviciu sau la angajarea într-un contract. Un exemplu în acest sens este cazul în care o bancă își monitorizează clienții într-o bază de date de credit de referință pentru a decide dacă să le ofere un împrumut.

În cele mai multe cazuri, un operator de date poate să considere că o prelucrare care îndeplinește două criterii ar necesita efectuarea unei DPIA. În general, WP29 consideră că, pe măsură ce sunt îndeplinite tot mai multe criterii de prelucrare, aceasta este mai susceptibilă să prezinte un risc ridicat pentru drepturile și libertățile persoanelor vizate și, prin urmare, să necesite o DPIA, indiferent de măsurile pe care operatorul intenționează să le adopte.

Cu toate acestea, în unele cazuri, **un operator de date poate considera că o prelucrare care îndeplinește numai unul dintre aceste criterii necesită o DPIA**.

Următoarele exemple ilustrează modul în care criteriile ar trebui să fie utilizate pentru a evalua dacă o anumită operațiune de prelucrare necesită o DPIA:

[17] A se vedea explicația din avizul WP29 privind limitarea scopului 13/EN WP 203;

Exemple de prelucrare	Criterii relevante posibile	Este DPIA susceptibilă să fie necesară?
Un spital care prelucrează datele genetice și de sănătate ale pacienților săi (sistem informatic din spitale).	- Date sensibile sau date foarte personale. - Date referitoare la persoanele vizate vulnerabile. - Date prelucrate la scară largă.	Da
Utilizarea unui sistem de camere pentru a monitoriza comportamentul de conducere pe autostrăzi. Operatorul intenționează să utilizeze un sistem inteligent de analiză video pentru a identifica autoturismele și pentru a recunoaște în mod automat plăcuțele de înmatriculare.	- Monitorizare sistematică. - Utilizarea inovatoare sau aplicarea unor soluții tehnologice sau organizaționale.	
O societate care monitorizează sistematic activitățile angajaților săi, inclusiv monitorizarea stațiilor de lucru, a activității pe internet a angajaților săi etc.	- Monitorizare sistematică. - Date referitoare la persoanele vizate vulnerabile.	
Colectarea de date publice de pe platformele de comunicare socială pentru generarea de profiluri.	- Evaluare sau punctare. - Date prelucrate pe scară largă. - Corelarea sau combinarea unor seturi de date. - Date sensibile sau date foarte personale:	
O instituție care creează o bază de date de rating de credit sau cu privire la frauda la nivel național.	- Evaluare sau punctare. - Luarea de decizii în mod automat cu un efect juridic sau similar semnificativ. - Împiedică persoana vizată să își exercite un drept sau să utilizeze un serviciu sau un contract. - Date sensibile sau date foarte personale:	
Stocarea în vederea arhivării de date trasabile devenite sensibile cu caracter personal pseudonimizate referitoare la persoanele vizate vulnerabile din cadrul proiectelor de cercetare sau din studiile clinice.	- Date sensibile: - Date referitoare la persoanele vizate vulnerabile. - Împiedică persoanele vizate să își exercite un drept sau să utilizeze un serviciu ori un contract.	
O prelucrare de „date cu caracter personal de la pacienți sau clienți de către un anumit medic, un alt profesionist în domeniul sănătății sau un avocat” (considerentul 91).	- Date sensibile sau date foarte personale. - Date referitoare la persoanele vizate vulnerabile.	Nu
O revistă online care utilizează o listă de distribuire pentru a trimite un abonament generic zilnic abonaților săi.	- Date prelucrate pe scară largă.	
Un site de vânzări online care afișează reclame pentru piese de schimb pentru autovehicule de epocă care implică crearea limitată de profiluri pe	- Evaluare sau punctare.	

Exemple de prelucrare	Criterii relevante posibile	Este DPIA susceptibilă să fie necesară?
baza articolelor vizualizate sau achiziționate pe propriul site.		

În schimb, o operațiune de prelucrare poate să corespundă cazurilor menționate mai sus și să fie considerată în continuare de către operator a nu fi „susceptibil[ă] să genereze un risc ridicat". În astfel de cazuri, operatorul ar trebui să justifice și să documenteze motivele pentru care nu a efectuat o DPIA și să includă/înregistreze avizele responsabilului cu protecția datelor.

În plus, ca parte a principiului responsabilității, fiecare operator de date „*păstrează o evidență a activităților de prelucrare desfășurate sub responsabilitatea lor*", inclusiv, printre altele, scopurile prelucrării, o descriere a categoriilor de date și a destinatarilor datelor și „*acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 32 alineatul (1)*" [articolul 30 alineatul (1)] și trebuie să analizeze susceptibilitatea unui risc ridicat, chiar dacă este posibil ca în cele din urmă acesta să nu efectueze o DPIA.

Notă: autoritățile de supraveghere sunt obligate să întocmească, să publice și să comunice o listă a operațiunilor de prelucrare care necesită o DPIA Comitetului european pentru protecția datelor (EDPB) [articolul 35 alineatul (4)][18]. Criteriile enunțate mai sus pot sprijini autoritățile de supraveghere să constituie o astfel de listă, cu un conținut mai specific adăugat în timp, dacă este cazul. De exemplu, prelucrarea oricărui tip de date biometrice sau a celor cu privire la copii ar putea fi considerată, de asemenea, ca fiind relevantă pentru dezvoltarea unei liste în conformitate cu articolul 35 alineatul (4).

b) Când nu este necesară o DPIA? Atunci când prelucrarea nu este „*susceptibil[ă] să genereze un risc ridicat*" sau atunci când există o DPIA similară, sau când aceasta a fost autorizată înainte de luna mai 2018, sau când aceasta are un temei juridic, sau se află pe lista operațiunilor de prelucrare pentru care nu este necesară o DPIA.

WP29 consideră că o DPIA nu este necesară în următoarele cazuri:

- **atunci când prelucrarea nu este „*susceptibil[ă] să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice*"** [articolul 35 alineatul (1)];
- **atunci când natura, domeniul de aplicare, contextul și scopurile prelucrării sunt foarte asemănătoare cu prelucrarea pentru care a fost efectuată o DPIA**. În astfel de cazuri, pot fi utilizate rezultatele DPIA pentru prelucrarea similară [articolul 35 alineatul (1)[19]];
- atunci când operațiunile de prelucrare au fost verificate de o autoritate de supraveghere înainte de luna mai 2018 în condiții specifice care nu s-au modificat[20] (a se vedea III.C);

[18] În acest context, „*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*" [articolul 35 alineatul (6)].

[19] „*O evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare*".

- **atunci când o operațiune de prelucrare,** în conformitate cu articolul 6 alineatul (1) litera (c) sau (e), **are un temei juridic** în dreptul Uniunii sau al unui stat membru, atunci când dreptul reglementează operațiunile specifice de prelucrare **și atunci când s-a efectuat deja o DPIA** în contextul elaborării respectivului temei juridic [articolul 35 alineatul (10)][21], cu excepția cazului în care un stat membru a declarat că este necesar să se efectueze o DPIA înainte de activitățile de prelucrare;
- **atunci când prelucrarea este inclusă pe lista opțională (stabilită de autoritatea de supraveghere) de operațiuni de prelucrare** pentru care nu este necesară o DPIA [articolul 35 alineatul (5)]. O astfel de listă poate cuprinde activități de prelucrare care sunt conforme cu respectivele condiții stabilite de către autoritate, în special prin intermediul orientărilor, al deciziilor sau al autorizațiilor specifice, al normelor privind conformitatea etc. (de exemplu în Franța, autorizații, excepții, norme simplificate, pachete de conformitate ...). În astfel de cazuri și sub rezerva reevaluării de către autoritatea de supraveghere competentă, o DPIA nu este necesară, dar numai în cazul în care prelucrarea se încadrează strict în domeniul de aplicare a procedurii relevante menționate în listă și continuă să respecte pe deplin toate cerințele relevante din GDPR.

C. <u>Dar în ceea ce privește operațiunile de prelucrare deja existente? DPIA sunt necesare în anumite circumstanțe.</u>

Cerința de a efectua o DPIA se aplică operațiunilor de prelucrare existente, susceptibile să genereze un risc ridicat la adresa drepturilor și a libertăților persoanelor fizice, în cazul cărora a avut loc o modificare a riscurilor, luând în considerare natura, domeniul de aplicare, contextul și scopurile prelucrării.

O DPIA nu este necesară în cazul operațiunilor de prelucrare care au fost verificate de către o autoritate de supraveghere sau de către responsabilul cu protecția datelor, în conformitate cu articolul 20 din Directiva 95/46/CE, și care sunt realizate într-un mod care nu s-a modificat de la verificarea prealabilă. Într-adevăr, „*deciziile adoptate ale Comisiei și autorizațiile autorităților de supraveghere emise pe baza Directivei 95/46/CE rămân în vigoare până când vor fi modificate, înlocuite sau abrogate*" (considerentul 171).

În schimb, acest lucru înseamnă că orice prelucrare de date ale cărei condiții de punere în aplicare (domeniu de aplicare, scop, datele cu caracter personal colectate, identitatea operatorilor de date sau a beneficiarilor, perioada de păstrare a datelor, măsuri tehnice și organizatorice etc.) s-au modificat de la verificarea prealabilă efectuată de autoritatea de supraveghere sau de responsabilul cu protecția datelor și sunt susceptibile să genereze un risc ridicat ar trebui să facă obiectul unei DPIA.

---

[20] „*Deciziile adoptate ale Comisiei și autorizațiile autorităților de supraveghere emise pe baza Directivei 95/46/CE rămân în vigoare până când vor fi modificate, înlocuite sau abrogate*" (considerentul 171).

[21] Atunci când o DPIA se efectuează în etapa de elaborare a unor acte legislative care prevăd un temei juridic pentru prelucrare, este probabil să se solicite o revizuire înainte de intrarea în funcțiune, întrucât legislația adoptată poate fi diferită de propunere în moduri care afectează aspectele legate de protecția vieții private și a datelor. În plus, este posibil să nu existe suficiente detalii tehnice disponibile cu privire la prelucrarea efectivă la momentul adoptării legislației, chiar dacă aceasta a fost însoțită de o DPIA. În astfel de cazuri, este posibil să fie necesară în continuare efectuarea unei DPIA specifice înainte de realizarea efectivă a activităților de prelucrare.

În plus, o DPIA ar putea fi necesară după o modificare a riscurilor rezultate în urma operațiunilor de prelucrare[22], de exemplu deoarece o nouă tehnologie a intrat în uz sau datele cu caracter personal sunt utilizate pentru un scop diferit. Operațiunile de prelucrare a datelor pot evolua rapid și pot apărea noi vulnerabilități. Prin urmare, ar trebui remarcat faptul că revizuirea unei DPIA este utilă nu numai pentru o îmbunătățire continuă ci, de asemenea, aceasta este esențială pentru a menține nivelul de protecție a datelor într-un mediu în schimbare de-a lungul timpului. O DPIA poate deveni necesară, de asemenea, deoarece contextul organizațional sau social pentru activitatea de prelucrare s-a modificat, de exemplu deoarece efectele anumitor decizii automatizate au devenit mai semnificative sau noi categorii de persoane vizate devin vulnerabile la discriminare. Fiecare dintre aceste exemple ar putea constitui un element care conduce la o modificare a riscului rezultat din activitatea de prelucrare în cauză.

În același timp, anumite modificări și-ar putea reduce riscul, de asemenea. De exemplu, o operațiune de prelucrare ar putea evolua astfel încât deciziile să nu mai fie automatizate sau în cazul în care o activitate de monitorizare nu mai este sistematică. În acest caz, revizuirea analizei de risc realizată poate demonstra că efectuarea unei DPIA nu mai este necesară.

Ca bună practică, **o DPIA ar trebui să fie revizuită în mod continuu și reevaluată în mod periodic**. Prin urmare, chiar dacă o DPIA nu este necesară la 25 mai 2018, va fi necesar, la momentul oportun, ca operatorul să efectueze o astfel de DPIA ca parte a obligațiilor sale de răspundere generală.

D. Cum se efectuează o DPIA?

a) În ce moment ar trebui să fie efectuată o DPIA? Înaintea prelucrării.

DPIA ar trebui să fie efectuată „*înaintea prelucrării*" [articolul 35 alineatele (1) și (10) și considerentele 90 și 93][23]. Aceasta este în concordanță cu asigurarea protecției datelor începând cu momentul conceperii și în mod implicit (articolul 25 și considerentul 78). DPIA ar trebui să fie văzută ca un instrument pentru sprijinirea procesului decizional în ceea ce privește prelucrarea.

DPIA ar trebui să înceapă cât mai curând posibil în elaborarea operațiunii de prelucrare, chiar dacă o parte din operațiunile de prelucrare încă nu sunt cunoscute. Actualizarea DPIA pe parcursul ciclului de viață a proiectului va asigura că protecția datelor și a vieții private este luată în considerare și va încuraja crearea de soluții care promovează respectarea normelor. De asemenea, poate fi necesară repetarea etapelor individuale ale evaluării pe măsură ce procesul de dezvoltare progresează, întrucât selectarea anumitor măsuri tehnice și organizatorice poate afecta severitatea sau probabilitatea riscurilor prezentate de prelucrarea datelor.

Faptul că DPIA ar putea necesita actualizare odată ce prelucrarea a început efectiv nu reprezintă un motiv valabil pentru amânarea sau neefectuarea unei DPIA. DPIA este un proces continuu, în special

[22] În ceea ce privește contextul, datele colectate, scopurile, funcționalitățile, datele cu caracter personal prelucrate, destinatarii, combinațiile de date, riscurile (active de sprijinire, sursele riscurilor, impactul potențial, amenințările etc.), măsurile de securitate și transferurile internaționale.

[23] Cu excepția cazului în care este vorba despre o prelucrare existentă deja, care a fost verificată în prealabil de autoritatea de supraveghere, caz în care DPIA ar trebui să fie efectuată înainte de realizarea unor modificări semnificative.

în cazul în care o operațiune de prelucrare este dinamică și în continuă schimbare. **Efectuarea unei DPIA este un proces continuu, nu un exercițiu unic.**

b) Cine este obligat să efectueze DPIA? Operatorul, împreună cu responsabilul cu protecția datelor și cu persoanele împuternicite de operator.

Operatorului îi revine responsabilitatea de a asigura efectuarea DPIA [articolul 35 alineatul (2)]. Efectuarea DPIA ar putea fi realizată de altă persoană, din interiorul sau din exteriorul organizației, însă operatorul rămâne responsabil în cele din urmă de această sarcină.

Operatorul trebuie să solicite, de asemenea, avizul responsabilului cu protecția datelor (DPO) în cazurile desemnate [articolul 35 alineatul (2)], iar acest aviz și deciziile luate de către operator ar trebui să fie documentate în cadrul DPIA. De asemenea, DPO ar trebui să monitorizeze funcționarea DPIA [articolul 39 alineatul (1) litera (c)]. Orientări suplimentare sunt furnizate în Orientările WP29 privind responsabilul cu protecția datelor 16/EN WP 243.

În cazul în care prelucrarea este efectuată integral sau parțial de către o persoană împuternicită de operator, **persoana împuternicită de operator ar trebui să asiste operatorul în efectuarea DPIA** și să furnizeze toate informațiile necesare [în conformitate cu articolul 28 alineatul (3) litera (f)].

Operatorul trebuie „*[să solicite] avizul persoanelor vizate sau al reprezentanților acestora*" [articolul 35 alineatul (9)] „*acolo unde este cazul*". WP29 consideră că:

- respectivele avize ar putea fi urmărite printr-o varietate de mijloace, în funcție de context (de exemplu, un studiu generic legate de scopul și mijloacele operațiunii de prelucrare, o întrebare pentru reprezentanții personalului sau sondaje uzuale transmise viitorilor clienți ai operatorului de date), asigurându-se că operatorul dispune de o bază legală pentru prelucrarea oricăror date cu caracter personal implicate în solicitarea unor astfel de avize. Cu toate acestea, ar trebui remarcat faptul că respectivul consimțământ pentru prelucrare în mod clar nu este o modalitate prin care să se solicite avizele persoanelor vizate;
- în cazul în care decizia finală a operatorului de date diferă de avizele persoanelor vizate, motivele acestuia de a continua sau nu ar trebui să fie documentate;
- de asemenea, operatorul ar trebui să își documenteze justificarea pentru nesolicitarea avizelor persoanelor vizate, în cazul în care decide că acest lucru nu este necesar, de exemplu în cazul în care acest lucru ar compromite caracterul confidențial al planurilor de afaceri ale societăților sau ar fi disproporționat sau imposibil de aplicat.

În cele din urmă, o bună practică este aceea de a defini și a documenta alte roluri și responsabilități specifice, în funcție de politica, procesele și normele interne, de exemplu:

- în cazul în care anumite unități operaționale pot propune efectuarea unei DPIA, respectivele unități ar trebui să furnizeze ulterior date DPIA și ar trebui să fie implicate în procesul de validare a DPIA;
- după caz, se recomandă solicitarea avizelor de la experți independenți din diferite profesii[24] (avocați, experți IT, experți în securitate, sociologi, etică etc.).
- rolurile și responsabilitățile persoanelor împuternicite de către operator trebuie să fie definite prin contract; iar DPIA trebuie să fie efectuată cu sprijinul persoanei împuternicite de către

[24] *Recomandări pentru un cadru de evaluare a impactului asupra vieții private pentru Uniunea Europeană, rezultatul D3:* http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

operator, ținând seama de natura prelucrării și de informațiile aflate la dispoziția persoanei împuternicite de operator [articolul 28 alineatul (3) litera (f)];

- responsabilul principal cu securitatea informațiilor (CISO), în cazul în care este desemnat, precum și responsabilul cu protecția datelor ar putea sugera ca operatorul să efectueze o DPIA cu privire la o operațiune specifică de prelucrare și ar trebui să sprijine părțile interesate în ceea ce privește metodologia, să contribuie la evaluarea calității evaluării cu privire la riscuri și a faptului dacă riscul rezidual este acceptabil, precum și să dezvolte cunoștințe specifice contextului operatorului de date;
- responsabilul principal cu securitatea informațiilor (CISO), în cazul în care este desemnat, și/sau departamentul IT ar trebui să acorde asistență operatorului și ar putea propune efectuarea unei DPIA cu privire la o operațiune de prelucrare specifică, în funcție de securitate sau de necesitățile operaționale.

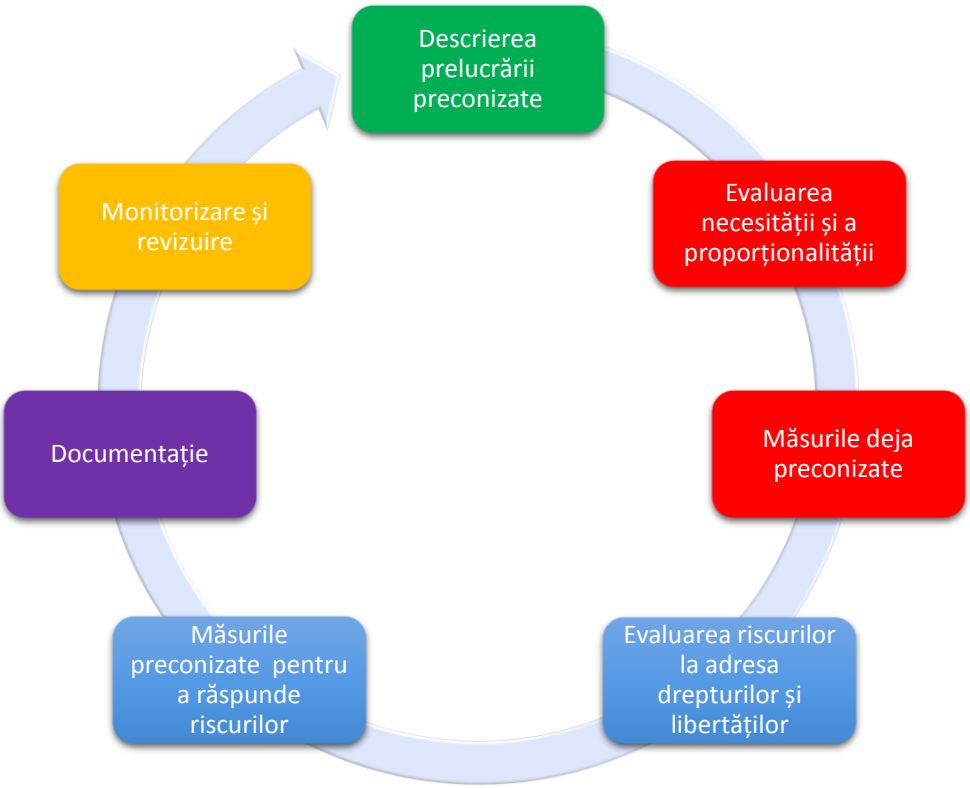
c) Care este metodologia de efectuare a unei DPIA? Metodologii diferite, dar criterii comune.

GDPR stabilește caracteristicile minime ale unei DPIA [articolul 35 alineatul (7) și considerentele 84 și 90]:

- „*o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării*";
- „*o evaluare a necesității și proporționalității operațiunilor de prelucrare*";
- „*o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate*";
- „*măsurile preconizate în vederea:*
  - „*abordării riscurilor*"*;*
  - „*să demonstreze conformitatea cu dispozițiile prezentului regulament*".

Figura de mai jos ilustrează procesul generic iterativ pentru efectuarea unei DPIA[25]:

[25] Ar trebui subliniat faptul că procesul descris aici este un proces iterativ: în practică, este probabil ca fiecare dintre aceste etape să fie reluată de mai multe ori înainte ca DPIA să poată fi finalizată.



Respectarea unui cod de conduită (articolul 40) trebuie să fie luată în considerare [articolul 35 alineatul (8)] atunci când se evaluează impactul unei operațiuni de prelucrare a datelor. Acest lucru poate fi util pentru a demonstra că au fost alese și puse în aplicare măsuri corespunzătoare, cu condiția ca respectivul cod de conduită să fie adecvat pentru operațiunea de prelucrare. De asemenea, ar trebui să fie luate în considerare certificările, sigiliile și mărcile pentru a demonstra conformitatea cu GDPR a operațiunilor de prelucrare efectuate de operatori și de persoanele împuternicite de operatori (articolul 42), precum și regulile corporatiste obligatorii (BCR).

Toate cerințele relevante stabilite în GDPR oferă un cadru amplu, generic pentru elaborarea și efectuarea unei DPIA. Punerea în aplicare practică a unei DPIA va depinde de cerințele stabilite în GDPR, care pot fi completate cu orientări practice mai detaliate. Prin urmare, punerea în aplicare a DPIA poate fi extinsă. Acest lucru înseamnă că inclusiv un operator mic de date poate elabora și pune în aplicare o DPIA care este adecvată pentru operațiunile sale de prelucrare.

Considerentul 90 din GDPR subliniază o serie de componente ale DPIA care se suprapun cu componente bine definite de gestionare a riscurilor (de exemplu, ISO 31000[26]). În ceea ce privește gestionarea riscurilor, evaluarea DPIA vizează „gestionarea riscurilor” pentru drepturile și libertățile persoanelor fizice, utilizând următoarele procese, prin:

- stabilirea contextului: „*având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și sursele riscului*”;

[26] Procese de gestionare a riscurilor: comunicare și consultare, stabilirea contextului, evaluarea riscurilor, tratarea riscurilor, monitorizarea și revizuirea (a se vedea termenii și definițiile, precum și cuprinsul, în previzualizarea ISO 31000: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

- evaluarea riscurilor: „*evaluării gradului specific de probabilitate a materializării riscului ridicat și gravitatea acestuia*”;
- tratarea riscurilor: „*atenuarea riscului respectiv*” și ”*asigurarea protecției datelor cu caracter personal*” și „*demonstrarea conformității cu prezentul regulament*”.

Notă: DPIA din cadrul GDPR este un instrument de gestionare a riscurilor pentru drepturile persoanelor vizate și, prin urmare, preia perspectivele acestora, astfel cum este cazul în anumite domenii (de exemplu, securitatea socială). Dimpotrivă, gestionarea riscurilor în alte domenii (de exemplu, securitatea informațiilor) se concentrează asupra organizației.

GDPR furnizează operatorilor de date flexibilitatea de a stabili structura și forma exactă a DPIA pentru a permite ca acestea să fie adaptate practicilor de lucru existente. Există o serie de procese diferite stabilite în cadrul UE și la nivel mondial care iau în considerare componentele descrise în considerentul 90. Cu toate acestea, indiferent de forma sa, o DPIA trebuie să fie o veritabilă evaluare a riscurilor, care permite operatorilor să ia măsuri pentru soluționarea acestora.

Metodologii diferite (a se vedea anexa 1 pentru exemple de metodologii privind protecția datelor și privind evaluarea impactului asupra vieții private) ar putea fi utilizate pentru a sprijini punerea în aplicare a cerințelor de bază prevăzute în GDPR. Pentru a permite existența acestor abordări diferite, făcând posibilă, în același timp, respectarea GDPR de către operatori, au fost identificate criterii comune (a se vedea anexa 2). Acestea clarifică cerințele de bază din regulament, dar oferă o marjă suficientă pentru diferite forme de punere în aplicare. Aceste criterii pot fi utilizate pentru a demonstra că o anumită metodologie DPIA îndeplinește standardele impuse de GDPR. **Este la latitudinea operatorului de date să aleagă o metodologie, însă această metodologie ar trebui să fie conformă cu criteriile prevăzute în anexa 2.**

WP 29 încurajează dezvoltarea de cadre DPIA sectoriale. Acest lucru se datorează faptului că astfel de cadre se pot baza pe cunoștințe sectoriale specifice, ceea ce înseamnă că DPIA poate aborda particularitățile unui anumit tip de operațiune de prelucrare (de exemplu, anumite tipuri de date, active corporatiste, potențiale impacturi, amenințări, măsuri). Acest lucru înseamnă că DPIA poate aborda problemele care apar într-un anumit sector economic sau atunci când se utilizează anumite tehnologii ori se efectuează anumite tipuri de operațiuni de prelucrare.

În cele din urmă, „*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*” [articolul 35 alineatul (11)[27]].

d) Există o obligația de a publica DPIA? Nu, însă publicarea unui rezumat ar putea spori încrederea, iar DPIA completă trebuie să fie comunicată autorității de supraveghere în cazul unei consultări prealabile sau dacă acest lucru este solicitat de către DPA.

Publicarea unei DPIA nu este o cerință legală a GDPR, fiind decizia operatorului dacă a face acest lucru. Cu toate acestea, operatorii ar trebui să ia în considerare publicarea cel puțin a unor părți, cum ar fi un rezumat sau o concluzie privind propria DPIA.

Scopul unui astfel de proces ar fi de a contribui la promovarea încrederii în operațiunile de prelucrare ale operatorului și de a demonstra responsabilitate și transparență. Publicarea unei DPIA este o bună

[27] Articolul 35 alineatul (10) exclude în mod explicit numai aplicarea articolului 35 alineatele (1)-(7).

practică în mod deosebit în cazul în care membrii publicului sunt afectați de operațiunea de prelucrare. Acesta ar putea fi cazul mai ales atunci când o autoritate publică efectuează o DPIA.

DPIA publicată nu trebuie să includă întreaga evaluare, în special atunci când DPIA ar putea prezenta informații specifice cu privire la riscuri de securitate pentru operatorul de date sau ar putea dezvălui secrete comerciale sau informații comerciale sensibile. În aceste condiții, versiunea publicată ar putea constitui doar un rezumat al principalelor concluzii ale DPIA sau chiar o declarație care atestă că a fost efectuată o DPIA.

În plus, în cazul în care o DPIA relevă riscuri reziduale ridicate, operatorul va trebui să solicite consultarea prealabilă pentru prelucrarea datelor din partea autorității de supraveghere [articolul 36 alineatul (1)]. Ca parte a acestui proces, DPIA trebuie să fie furnizată în întregime [articolul 36 alineatul (3) litera (e)]. Autoritatea de supraveghere poate să își furnizeze avizul[28] fără a compromite secretele comerciale sau a dezvălui vulnerabilități de securitate, sub rezerva principiilor aplicabile în fiecare stat membru cu privire la accesul public la documentele oficiale.

E. Când se consultă autoritatea de supraveghere? Atunci când riscurile reziduale sunt ridicate.

Astfel cum s-a explicat mai sus:

- O DPIA este necesară atunci când o operațiune de prelucrare „*este susceptibil[ă] să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice*" [articolul 35 alineatul (1), a se vedea secțiunea III.B.a]. De exemplu, prelucrarea pe scară largă a datelor de sănătate este considerată ca fiind susceptibilă să genereze un risc ridicat și necesită o DPIA;
- ulterior, operatorului de date îi revine responsabilitate de a evalua riscurile pentru drepturile și libertățile persoanelor vizate și de a identifica măsurile[29] preconizate pentru a reduce aceste riscuri la un nivel acceptabil și pentru a demonstra conformitatea cu GDPR [articolul 35 alineatul (7), a se vedea secțiunea III.C.c). Pentru stocarea datelor cu caracter personal pe calculatoare portabile, un exemplu ar putea fi utilizarea unor măsuri de securitate tehnice și organizaționale adecvate (criptarea completă efectivă a discului, gestionarea fiabilă a parolelor, controlul adecvat al accesului, copii de rezervă securizate etc.) în plus față de politicile existente (aviz, consimțământ, dreptul de acces, dreptul de a formula obiecții etc.).

În exemplul de mai sus cu privire la laptop, în cazul în care se consideră că riscurile au fost reduse suficient de către operatorul de date și ca urmare a interpretării articolului 36 alineatul (1) și a considerentelor 84 și 94, prelucrarea poate fi efectuată fără consultarea cu autoritatea de supraveghere. În cazurile în care riscurile identificate nu pot fi abordate în mod suficient de operatorul de date (și anume, riscurile reziduale rămân ridicate), atunci operatorul de date trebuie să consulte autoritatea de supraveghere.

Un exemplu de risc rezidual ridicat inacceptabil include situații în care persoanele vizate pot suporta consecințe semnificative sau chiar ireversibile, pe care nu le pot depăși (de exemplu: accesul ilegal la date care conduce la o amenințare pentru viețile persoanelor vizate, o disponibilizare, un pericol

[28] Avizul scris adresat operatorului este necesar numai atunci când autoritatea de supraveghere consideră că prelucrarea prevăzută nu este conformă cu regulamentul, în conformitate cu articolul 36 alineatul (2).

[29] Inclusiv luând în considerare orientările existente din partea Comitetului european pentru protecția datelor și a autorităților de supraveghere și ținând seama de stadiul actual al tehnologiei și costurile de punere în aplicare, astfel cum se prevede la articolul 35 alineatul (1).

financiar) și/sau atunci când pare evident că riscul va avea loc (de exemplu, prin incapacitatea de a reduce numărul persoanelor care accesează datele din cauza partajării, a utilizării sau a modurilor de distribuție a acestora sau atunci când o vulnerabilitate binecunoscută nu este remediată).

Ori de câte ori operatorul de date nu poate identifica suficiente măsuri pentru a reduce riscurile la un nivel acceptabil (și anume, riscurile reziduale sunt în continuare ridicate), consultarea cu autoritatea de supraveghere este obligatorie[30].

În plus, operatorul va trebui să se consulte cu autoritatea de supraveghere ori de câte ori legislația statului membru impune operatorilor să se consulte cu aceasta și/sau să obțină în prealabil autorizarea din partea acesteia în legătură cu prelucrarea de către un operator în vederea îndeplinirii unei sarcini exercitate de acesta în interes public, inclusiv prelucrarea în legătură cu protecția socială și sănătatea publică [articolul 36 alineatul (5)].

Cu toate acestea, ar trebui remarcat faptul că, indiferent dacă această consultare a autorității de supraveghere este sau nu obligatorie în funcție de nivelul de risc rezidual, rămân valabile obligațiile de păstrare a unei evidențe a DPIA și de actualizare în timp util a DPIA.

IV. Concluzii și recomandări

DPIA reprezintă o modalitate utilă pentru operatorii de date de a pune în aplicare sisteme de prelucrare a datelor care sunt conforme cu GDPR și pot fi obligatorii pentru anumite tipuri de operațiuni de prelucrare. Acestea pot fi extinse și pot lua forme diferite, iar GDPR stabilește cerințele de bază ale unei DPIA eficace. Operatorii de date ar trebui să considere efectuarea unei DPIA ca fiind o activitate utilă și pozitivă care sprijină respectarea legislației.

Articolul 24 alineatul (1) stabilește responsabilitatea principală a operatorului în ceea ce privește conformitatea cu GDPR: „*[ț]inând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament. Respectivele măsuri se revizuiesc și se actualizează dacă este necesar*”.

DPIA reprezintă un element-cheie pentru respectarea regulamentului în cazul în care este planificată sau are loc o prelucrare de date cu risc ridicat. Acest lucru înseamnă că operatorii de date ar trebui să utilizeze criteriile prevăzute în prezentul document pentru a stabili dacă trebuie sau nu să fie efectuată o DPIA. Politica internă a operatorului de date ar putea extinde această listă dincolo de cerințele legale ale GDPR. Acest lucru ar trebui să conducă la creșterea încrederii în rândul persoanelor vizate și al altor operatori de date.

În cazul în care este planificată o prelucrare cu un posibil risc ridicat, operatorul de date trebuie:

- să aleagă o metodologie DPIA (exemple sunt prezentate în anexa 1) care să satisfacă criteriile de la anexa 2 sau să precizeze și să pună în aplicare un proces sistematic privind DPIA care:
  - este în conformitate cu criteriile din anexa 2;

[30] Notă: „*pseudonimizarea și criptarea datelor cu caracter personal*” (precum și minimizarea datelor, mecanismele de supraveghere etc.) nu sunt în mod neapărat măsuri adecvate. Acestea sunt doar exemple. Măsurile necesare depind de context și de riscuri, care sunt specifice operațiunilor de prelucrare.

    - este integrat în procesele existente de elaborare, de dezvoltare, de modificare, de revizuire a riscurilor și operaționale în conformitate cu procesele interne, contextul și cultura;
    - implică părțile interesate relevante și definește în mod clar responsabilitățile care le revin (operator, DPO, persoane vizate sau reprezentanții acestora, întreprinderi, servicii tehnice, persoane împuternicite de către operator, responsabilul cu securitatea informațiilor etc.);
- să furnizeze raportul DPIA autorității de supraveghere competente atunci când acest lucru este necesar;
- să consulte autoritatea de supraveghere în cazul în care nu reușește să stabilească suficiente măsuri pentru a atenua riscurile ridicate;
- să revizuiască periodic DPIA și prelucrarea pe care o evaluează, cel puțin atunci când are loc o modificare a riscului reprezentat de operațiunea de prelucrare;
- să documenteze deciziile luate.

Anexa 1 – Exemple de cadre DPIA existente din UE

GDPR nu precizează procesul DPIA care trebuie să fie urmat, ci permite, în schimb, operatorilor de date să introducă un cadru care completează practicile lor de lucru existente, cu condiția ca acesta să ia în considerare componentele descrise la articolul 35 alineatul (7). Un astfel de cadru poate fi adaptat la operatorul de date sau poate fi comun într-o anumită industrie. Cadrele publicate anterior elaborate de DPA din UE și cadrele sectoriale ale UE cuprind (dar nu se limitează la):

Exemple de cadre generice din UE:

- DE: Modelul standard pentru protecția datelor, V.1.0 – Versiune de probă, 2016[31].
  https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014.
  https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: *Evaluarea impactului asupra vieții private (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
  https://www.cnil.fr/fr/node/15798
- REGATUL UNIT: *Cod de practică pentru efectuarea de evaluări ale impactului asupra vieții private*, Biroului Comisarului pentru Informații (ICO), 2014.
  https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Exemple de cadre sectoriale din UE:

- Cadrul pentru evaluarea impactului asupra protecției datelor și a vieții private pentru aplicațiile RFID[32].
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Modelul de evaluare a impactului asupra protecției datelor pentru sistemele de rețele inteligente și de contorizare inteligentă[33]
  http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

---

[31] Recunoscut în mod unanim și afirmativ (în conformitate cu abținerea din Bavaria) de cele 92. Conferința autorităților independente de protecție a datelor din Bund și Länder în Kühlungsborn în perioada 9-10 noiembrie 2016.

[32] A se vedea, de asemenea::

- Recomandarea Comisiei din 12 mai 2009 privind aplicarea principiilor de respectare a vieții private și protecție a datelor în aplicațiile bazate pe identificarea prin radiofrecvență.
  https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- Avizul 9/2011 privind propunerea revizuită a sectorului industrial referitoare la un cadru de evaluare a impactului aplicațiilor RFID asupra protecției vieții private și a datelor.
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_ro.pdf

[33] A se vedea, de asemenea, Avizul nr. 07/2013 privind modelul de evaluare a impactului asupra protecției datelor pentru sistemele de rețele inteligente și de contorizare inteligentă („modelul DPIA") pregătit de Grupul de experți nr. 2 al Grupului operativ pentru rețelele inteligente din cadrul Comisiei.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_ro.pdf

Un standard internațional va furniza, de asemenea, orientări pentru metodologiile utilizate pentru efectuarea unei DPIA (ISO/IEC 29134[34]).

[34] ISO/IEC 29134 (project), *Tehnologia informației — Tehnici de securitate —Evaluarea impactului asupra vieții private* — Orientări, Organizația Internațională de Standardizare (ISO).

Anexa 2 – Criterii pentru o DPIA acceptabilă

WP29 propune următoarele criterii pe care operatorii de date le pot utiliza pentru a determina dacă o DPIA sau o metodologie pentru efectuarea unei DPIA este suficient de cuprinzătoare pentru a respecta GDPR:

- ☐ este furnizată o descriere sistematică a prelucrării [articolul 35 alineatul (7) litera (a)]:
  - ☐ natura, domeniul de aplicare, contextul și scopurile prelucrării sunt luate în considerare (considerentul 90);
  - ☐ sunt înregistrate datele cu caracter personal, destinatarii și perioada pentru care datele cu caracter personal vor fi stocate;
  - ☐ este furnizată o descriere funcțională a operațiunii de prelucrare;
  - ☐ sunt identificate activele pe care se bazează datele cu caracter personal (hardware, software, rețele, persoane, hârtia sau canalele de transmisie a hârtiei);
  - ☐ respectarea codurilor de conduită aprobate este luată în considerare [articolul 35 alineatul (8)];
- ☐ necesitatea și proporționalitatea sunt evaluate [articolul 35 alineatul (7) litera (b)]:
  - ☐ sunt stabilite măsurile avute în vedere pentru respectarea regulamentului [articolul 35 alineatul (7) litera (d) și considerentul 90], luând în considerare:
    - ☐ măsurile care contribuie la proporționalitatea și necesitatea prelucrării pe baza:
      - ☐ scopului sau a scopurilor determinate, explicite și legitime [articolul 5 alineatul (1) litera (b)];
      - ☐ legalității prelucrării (articolul 6);
      - ☐ datelor adecvate, relevante și limitate la ceea ce este necesar [articolul 5 alineatul (1) litera (c)];
      - ☐ duratei limitate legate de stocare [articolul 5 alineatul (1) litera (e)];
    - ☐ măsurile care contribuie la drepturile persoanelor vizate:
      - ☐ informațiile furnizate persoanei vizate (articolele 12, 13 și 14);
      - ☐ dreptul de acces și dreptul la portabilitatea datelor (articolele 15 și 20);
      - ☐ dreptul la rectificare și dreptul la ștergere (articolele 16, 17 și 19);
      - ☐ dreptul la opoziție și la restricționarea prelucrării (articolele 18, 19 și 21);
      - ☐ relațiile cu persoanele împuternicite de operator (articolul 28);
      - ☐ garanțiile privind transferul (transferurile) internațional(e) (capitolul V);
      - ☐ consultarea prealabilă (articolul 36).
- ☐ riscurile pentru drepturile și libertățile persoanelor vizate sunt gestionate [articolul 35 alineatul (7) litera (c)]:
  - ☐ originea, natura, specificitatea și gravitatea riscurilor sunt evaluate (a se vedea considerentul 84) sau, mai precis, pentru fiecare risc (accesul nelegitim, modificările nedorite și dispariția de date) din punctul de vedere al persoanelor vizate:
    - ☐ sursele riscurilor sunt luate în considerare (considerentul 90);
    - ☐ impacturile potențiale pentru drepturile și libertățile persoanelor vizate sunt identificate în cazul unor evenimente nedorite, inclusiv accesul nelegitim, modificarea nedorită și dispariția de date;
    - ☐ amenințările care ar putea conduce la accesul nelegitim, modificări nedorite și dispariția de date sunt identificate;
    - ☐ probabilitatea și gravitatea sunt estimate (considerentul 90);
  - ☐ măsurile preconizate în vederea abordării respectivelor riscuri sunt determinate [articolul 35 alineatul (7) litera (d) și considerentul 90];
- ☐ părțile interesate sunt implicate:
  - ☐ avizul DPO este solicitat [articolul 35 alineatul (2)];

- ☐ avizele persoanelor vizate sau ale reprezentanților acestora sunt solicitate, dacă este cazul [articolul 35 alineatul (9)].