GRUPUL DE LUCRU „ARTICOLUL 29” PENTRU PROTECȚIA DATELOR

17/RO

WP 248 rev.01

Ghid privind Evaluarea impactului asupra protecției datelor (DPIA) și stabilirea dacă o prelucrare este „susceptibilă să genereze un risc ridicat” în sensul Regulamentului 2016/679

Adoptat în data de 4 aprilie 2017

Revizuit și adoptat în data de 4 octombrie 2017

Acest grup de lucru a fost creat în temeiul articolului 29 din Directiva 95/46/CE și este un organism consultativ european independent care se ocupă cu protecția și confidențialitatea datelor. Sarcinile sale sunt descrise la articolul 30 din Directiva 95/46/CE și la articolul 15 din Directiva 2002/58/CE.

Secretariatul este asigurat de Direcția C (Drepturi fundamentale și cetățenia Uniunii) din cadrul Comisiei Europene, Direcția Generală Justiție și Consumatori, B- 1049 Bruxelles, Belgia, biroul MO-59 05/35.

Adresa web: http://ec.europa.eu/justice/data-protection/index_en.htm

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 directiva respectivă,

având în vedere regulamentul său de procedură,

ADOPTĂ PREZENTUL GHID:

CUPRINS

I. INTRODUCERE

Regulamentul 2016/679[1] (RGPD) va deveni aplicabil începând cu data de 25 mai 2018. Art. 35 din RGPD introduce conceptual de Evaluarea impactului asupra protecției datelor (DPIA[2]), așa cum prevede și Directiva 2016/680[3].

DPIA este un process destinat să descrie prelucrarea, să evalueze necesitatea și proporționalitatea acesteia și să contribuie la gestionarea riscurilor la adresa drepturilor și libertăților persoanelor vizate rezultate din prelucrarea datelor cu caracter personal[4], prin evaluarea acestora și stabilirea de măsuri pentru atenuarea lor. DPIA reprezintă un instrument important pentru responsabilizare deoarece ajută operatorii de date nu numai să respecte cerințele RGPD, ci și să demonstreze că au fost luate măsuri adecvate pentru a asigura conformitatea cu Regulamentul (a se vedea de asemenea și Art. 24)[5]. Cu alte cuvinte, **DPIA reprezintă un proces pentru construirea și demonstrarea conformității.**

Potrivit RGPD, nerespectarea cerințelor DPIA poate conduce la aplicarea de amenze de către autoritatea de supraveghere. Nerealizarea unei DPIA atunci când prelucrarea face obiectul unei DPIA (art. 35 (1) și (3) - (4)), realizarea unei DPIA într-un mod incorect (art. 35 (2) și (7) – (9)) sau dacă nu se consultă cu autoritatea de supraveghere competentă, dacă este cazul (art. 36 (3) litera (e)), poate conduce la o amendă administrativă de până la 10 milioane EUR sau, în cazul unei întreprinderi, până la 2% din cifra de afaceri globală anuală, oricare dintre acestea este mai mare.

II. OBIECTIVUL GHIDULUI

[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 protecției datelor" (DPIA) este adesea folosit în alte contexte pentru a se referi la același concept.

[3] Art. 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 că o evaluare de impact asupra protecției datelor este necesară pentru „*prelucrarea care este susceptibilă să genereze un risc ridicat petnru drepturile și libertățile persoanelor fizice*".

[4] RGPD nu definește în mod formal conceptual de DPIA ca atare, dar

- este specificat conținutul său minim în art. 35 (7), după cum urmează:
  - o „*(a) o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;*
  - o *(b) o evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri;*
  - o *(c) o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate menționate la alin. (1); și*
  - o *(d) măsurile preconizate în vedere 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 său 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 evalueze, 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*".

Prezentul ghid ia în considerare:

- Declarația Grupului de Lucru Articolul 29 14/EN WP 218[6];
- Ghidul Grupului de Lucru Articolul 29 privind responsabilul cu protecția datelor 16/EN WP 243[7];
- Opinia Grupului de Lucru Articolul 29 privind limitarea scopului 13/EN WP 203[8];
- standardele internaționale[9].

În conformitate cu abordarea bazată pe risc, implementată de RGPD, realizarea unei DPIA nu este obligatorie pentru fiecare operațiune de prelucrare. DPIA este necesară numai atunci când prelucrarea este „susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice" (art. 35 (1)). Pentru a asigura o interpretare consecventă a circumstanțelor în care o DPIA este obligatorie (art. 35 (3)], prezentul ghid vizează, în primul rând, clarificarea acestei noțiuni și furnizarea de criterii pentru listele care urmează să fie adoptate de autoritățile de protecție a datelor (DPA) în temeiul art. 35 (4).

Potrivit art. 70 (1) (e), Comitetul European pentru Protecția Datelor (EDPB) va putea emite ghiduri, recomandări și bune practici pentru a încuraja o aplicarea consecventă a RGPD. Obiectivul prezentului document este de a anticipa o astfel de activitate viitoare a EDPB și, prin urmare, de a clarifica dispozițiile relevante ale RGPD pentru a veni în ajutorul operatorilor de date să respecte legea și pentru a foeri certitudine juridică operatorilor de date care sunt obligați să efectueze DPIA.

Acest Ghid caută se promoveze elaborarea:

- unei liste comune la nivelul UE a operațiunilor de prelucrare pentru care DPIA este obligatorie (art. 35 (4));
- unei liste comune la nivelul UE a operațiunilor de prelucrare pentru care DPIA nu este necesară (art. 35(5));
- criterii comune privind metodologia pentru realizarea unei DPIA (art. 35(5));
- criterii comune pentru menționarea situațiilor în care autoritatea de supraveghere va fi consultată (art. 36(1));
- recomandări, acolo unde este posibil, pe baza experienței dobândite în statele membre UE.

III. DPIA: EXPLICAT DE REGULAMENT

[6] Declarația Grupului de Lucru Articolul 29 14/EN WP 218 cu privire la rolul unei abordări bazate pe riscuri pentru cadrul legal în domeniul protecției datelor, adoptată în data de 30 mai 2014.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

[7] Ghidul Grupului de Lucru Articolul 29 privind responsabilul cu protecția datelor WP 243, adoptat în data de 13 decembrie 2016.
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[8] Opinia Grupului de Lucru Articolul 29 03/2013 privind limitarea scopului 13/EN WP 203, adoptată în data de 2 aprilie 2013.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[9] Spre exemplu ISO 31000:2009, *Managementul riscului – Principii și linii directoare*, Organizația Internațională de Standardizare (ISO); ISO/IEC 29134 (proiect), *Tehnologia informației – Tehnici de securitate – Evaluare de impact asupra protecției datelor – Ghid,* Organizația Internațională de Stardardizare (ISO).

RGPD cere operatorilor să implementeze măsuri adecvate pentru a asigura și demonstra conformitatea cu RGPD, luând în considerare, printre altele, „riscurile de variație a probabilității și gravității asupra drepturilor și libertăților persoanelor fizice” (art. 24(1)). Obligația operatorilor de a realiza DPIA în anumite situații ar trebui înțeleasă în contextul obligației lor generale de a gestiona în mod corespunzător riscurile[10] prezentate de prelucrarea datelor cu caracter personal.

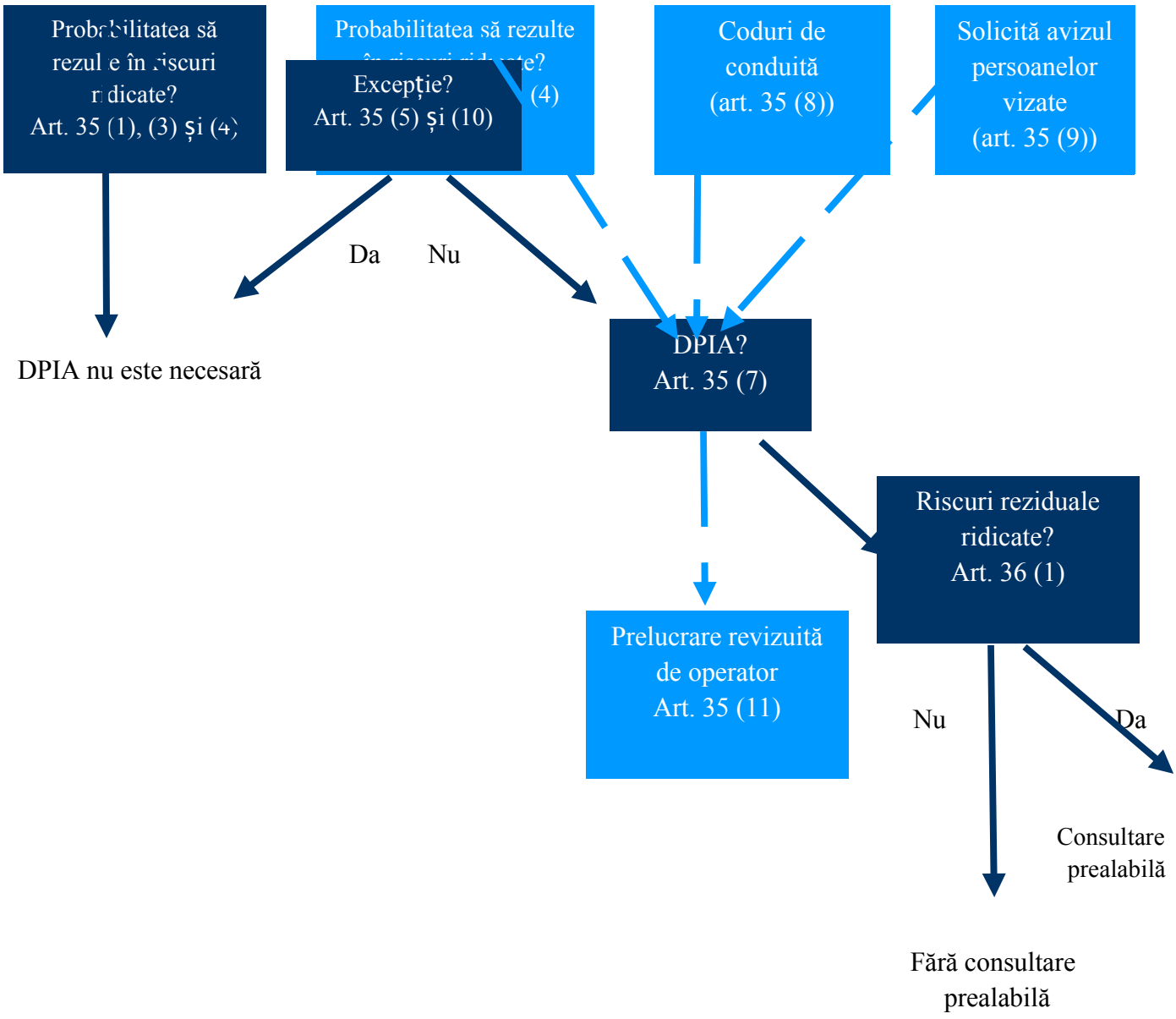
Un „risc” reprezintă un scenariu care descrie un eveniment și consecințele acestuia, estimat în termeni de severitate și probabilitate. Pe de altă parte, „managementul riscului” poate fi definit ca fiind activitățile coordonate pentru a conduce și controla o organizație cu privire la un risc.

Art. 35 se referă la un risc probabil ridicat „pentru drepturile și libertățile persoanelor”. Așa cum se menționează și în Declarația Grupului de Lucru Articolul 29 privind rolul unei abordări bazate pe riscuri în ceea ce privește cadrul juridic privind protecția datelor, trimiterea la „drepturile și libertățile” persoanelor vizate se referă în primul rând la drepturile la protecția date lor și a vieții private, dar poate implica și alte drepturi fundamentale precum libertatea de exprimare, libertatea de gândire, libertatea de mișcare, interzicerea discriminării, dreptul la libertate, conștiință și religie.

În conformitatea cu abordarea bazată pe risc implementată de RGPD, realizarea unei DPIA nu este obligatorie pentru fiecare operațiune de prelucrare. În schimb, DPIA este necesară numai în cazul în care un tip de prelucrare „ar putea duce la un risc ridicat petnru drepturile și libertățile persoanelor fizice” (art. 35(1)). Simplul fapt că condițiile care declanșează obligația de a realiza DPIA nu au fost îndeplinite nu diminuează, însă, obligația generală a operatorilor de a implementa măsuri corespunzătoare pentru gestionarea adecvată a riscurilor asupra drepturilor și libertăților persoanelor vizate. În practică, acest lucru înseamnă că operatorii trebuie să evalueze în mod continuu riscurile create de activităților lor de prelucrare pentru a identifica monentul în care un tip de prelucrare „ar putea duce la un risc ridicat pentru drepturile și libertățile persoanelor fizice”.

Figura următoare ilustrează principiile de bază referitoare la DPIA din RGPD:

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



A. Cui se aplică DPIA? Unei singure operațiuni de prelucrare sau unui set de operațiuni similare de prelucrare

DPIA se poate referi doar la o singură operațiune de prelucrare. Cu toate acestea, art. 35 (1) menționează că „*o evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicată similare*”. Considerentul 92 adaugă faptul că „*există situații 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 organismte 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 orizontată utilizată la scară largă*”.

O singură DPIA poate fi folosită pentru a evalua multiple operațiuni de prelucrare similare în ceea ce privește natura, obiectivul, contextul, scopul și riscurile. Într-adevăr, DPIA urmărește să studieze în mod sistematic situații noi care ar putea conduce la riscuri ridicate pentru drepturile și libertățile

persoanelor fizice și nu este necesară realizarea unei DPIA în cazurile (adică operațiunile de prelucrare efectuate într-un context specific și pentru un anumit scop) care au fost deja studiate. Acest lucru ar putea fi situația în care se utilizează o tehnologie similară pentru a colecta aceleași tip de date în aceleași scopuri. De exemplu, un grup de autorități municipale care instituie fiecare un sistem CCTV similar ar putea realiza o singură DPIA care să acopere prelucrarea efectuată de acești operatori separați sau un operator feroviar (un singur operator) ar putea acoperi supravegherea video în toate stațiile sale de cale ferată cu o singură DPIA. Acest lucru poate fi, de asemenea, aplicabil operațiunilor de prelucrare similare implementate de diverși operatori de date. În aceste situații, o DPIA de referință ar trebui împărțită sau pusă la dispoziția publicului, măsurile descrise în DPIA trebuie puse în aplicare și trebuie furnizată o justificare pentru realizarea unei DPIA unice.

În situația în care operațiunea de prelucrare implică operatori asociații, aceștia trebuie să-și definească exact obligațiile. DPIA trebuie să stabilească partea responsabilă pentru diferitele măsuri destinate să trateze riscurile și să protejeze drepturile și libertățile pesoanelor vizate. Fiecare operator de date ar trebui să-și exprime nevoile și să împărtășească informații utile fără a compromite secretele (spre exemplu: protecția secretelor comerciale, a proprietății intelectuale, a informațiilor comerciale) sau a dezvălui vulnerabilități.

O DPIA poate fi, de asemenea, utilă pentru evaluarea impactului asupra protecției datelor a unui produs tehnologic, de exemplu un hardware sau software, în cazul în care acest lucru este probabil să fie utilizat de diferiți operatori de date pentru a efectua diferite operațiuni de prelucrare. Bineînțeles, operatorul de date care utilizează produsul rămâne obligat să-și îndeplinească propria DPIA în ceea ce privește implementarea specifică, dar acesta poate fi informat în legătură cu o DPIA pregătită de furnizorul de produse, dacă este cazul. Un exemplu ar putea fi relația dintre producătorii de contoare inteligente și companiile de utilități. Fiecare furnizor sau procesator de produs ar trebui să împărtășească informații utile fără a compromite vreun secret și fără a aduce riscuri de securitate prin divulgarea vulnerabilităților.

B. <u>Care operațiuni de prelucrare fac obiectul unei DPIA? În afară de excepții, situațiile care sunt „susceptibile să genereze un risc ridicat”</u>

Prezenta secțiune descrie când este și când nu este necesară realizarea unei DPIA.

Cu excepția cazului în care operațiunea de prelucrare se încadrează într-o excepție (III.B.a), trebuie să se efectueze o DPIA în cazul în care o operațiune de prelucrare este „*susceptibilă să genereze un risc ridicat*” (III.B.b).

a) Când este obligatorie DPIA? Când prelucrarea este „susceptibilă să genereze un risc ridicat”

GDPR nu impune efectuarea unei DPIA pentru fiecare operațiune de prelucrare care poate conduce la riscuri pentru drepturile și libertățile persoanelor fizice. Executarea unei DPIA este obligatorie numai atunci când prelucrarea este „susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice” (art. 35 (1), ilustrat de art. 35 (3) și completat de art. 35 (4)). Este deosebit de relevant atunci când se introduce o nouă tehnologie de prelucrare a datelor[11].

În situațiile în care nu este clar dacă DPIA este obligatorie, Grupul de Lucru Articolul 29 recomandă, totuși, efectuarea unei DPIA ca un instrument util pentru a ajuta operatorii de date să respecte legea privind protecția datelor.

[11] A se vedea Considerentele 89, 91 și art. 35 (1) și (3) pentru alte exemple.

Chiar dacă DPIA ar putea fi solicitată în alte circumstanțe, art. 35 (3) oferă câteva exemple atunci când o operațiune de prelucrare este „susceptibilă să genereze riscuri ridicate":

- „*(a) evaluare sistematică și cuprinzătoare a aspectelor persoanle 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 peroana fizică sau care o afectează în mod similar într-o măsură semnificativă*[12]*;*
- *(b) prelucrarea pe scară largă a unor categorii speciale de date, menționată la art. 9 (1) sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționat la art. 10*[13]*; sau*
- *(c) monitorizare sistematică pe cară largă a unei zone accesibilte publicului"*.

După cum indică expresia „în special" din teza introductivă a art. 35 (3) din RGPD, aceasta este o listă neexhaustivă. Pot exista operațiuni de prelucrare „cu risc ridicat" care nu sunt cuprinse în această listă, dar prezintă totuși riscuri la fel de mari. Aceste operațiuni de prelucrare ar trebui, de asemenea, să facă obiectul DPIA. Din acest motiv, criteriile prezentate mai jos depășesc uneori o explicație simplă a ceea ce ar trebui înțeles prin cele trei exemple menționate la art. 35 (3) din RGPD.

Pentru a oferi un set mai precis de operațiuni de prelucrare care necesită o DPIA datorită riscului ridicat inerent, ținând seama de elementele speciale ale art. 35 (1) și ale art. 35 (3) a)-c), la adoptarea la nivel național a listei în conformitate cu art. 35 (4) și Considerentele 71, 75 și 91 și alte referințe RGPD la operațiunile de prelucrare „susceptibile să conducă la un risc ridicat"[14] trebuie luate în considerare următoarele nouă criterii.

1. 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 comportabment sau de marketing bazat pe utilizarea sau navigarea pe site-ul său web.
2. Proces decizional automatizat cu efecte legale sau similare semnificative: prelucrare care vizează luarea deciziilor asupra persoanelor vizate care produc „*efecte juridice privind prsoana 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.
3. 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

[12] A se vedea Considerentul 71: „*în special în vederea analizării sau preconizării anumitor aspecte privind randamentul la locul de muncă al persoanei vizate, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea su comportamentul, locația sau deplasările, pentru a crea sau utiliza profilurile 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 și sunt prelucrate date genetice, date privind starea de sănătate sau orientare sexuală sau condamnările penale și infracțiuni sau măsuri de securitate conexe*".

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

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.

4. Date sensibile sau date de natură foarte personală: acestea includ categorii speciale de date cu caracter personal așa cum sunt definite în art. 9 (spre exemplu informații privind opiniile politice al persoanelor fizice), precum și date cu caracter personal privind condamnările penale sau infracțuni așa cum sunt definite în art. 10. 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. Aceste date cu caracter personal sunt considerate ca fiind date sensibile (deoarece acest termen este înțeles în mod obișnuit) deoarece sunt legate de activitățile casnice și private (cum ar fi comunicațiile electronice a căror confidențialitate ar trebui protejată) sau deoarece respectivele date influențează exercitarea unui drept fundamental (cum ar fi datele de localizare a căror colectare pune la îndoială libertatea de mișcare) sau pentru că încălcarea lor implică în mod clar efecte grave asupra vieții de zi cu zi a persoanei vizate (cum ar fi 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, date cum ar fi documentele personale, e-mailurile, jurnalele, notele de la cititorii electronici echipate cu funcții de notare și informații foarte personale conținute în aplicațiile de log.
5. 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]:
    a. numărul persoanelor vizate, ori un număr exact ori un procent din populația relevantă;
    b. volumul datelor și/sau gama de elemente diferite de date în curs de prelucrare;
    c. durata sau permanența activității de prelucrare a datelor;
    d. suprafața geografică a activității de prelucrare.
6. 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[17].
7. 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. Persoanele vizate vulnerabile pot include copiii (pot fi considerați incapabili să se opună sau să consimtă sau să se opună în mod deliberat la prelucrarea datelor lor), angajați, segmente mai vulnerabile ale populației care necesită protecție specială (persoane bolnave, solicitanți de azil sau vârstnici, pacienți etc.) și, în orice caz, poate fi identificat un dezechilibru în relația dintre poziția persoanei vizate și operator.

---

[15] Grupul de Lucru Articoul 29 interpretează „*sistematic*" în sensul unei sau mai multora dintre (a se vedea Ghidul Grupului de Lucru Articoul 29 privind responsabilul cu protecția datelor 16/EN WP 243):

- care apare în conformitate cu un sistem;
- prearanjat, organizat sau metodic;
- care are loc în cadrul unui plan general de colectare a datelor;
- realizat ca parte a unei strategii.

Grupul de Lucru Articolul 29 interpretează „*zonă accesibilă publicului*" ca fiind orice loc deschis oricărui membru a publicului, de exemplu o piațetă, un centru comercial, o stradă, o piață, o gară sau o bibliotecă publică.

[16] A se vedea Ghidul Grupului de Lucru Articolul 29 privind responsabilul cu protecția datelor 16/EN WP 243.

[17] A se vedea explicația din Opinia Grupului de Lucru Articolul 29 privind limitarea scopului 13/EN WP 203, pg.24.

8. 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 jpoate implica noi forme de colectare și utilizarea a datelor, eventual cu un risc ridicat petnru 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 cotidinene și a vieții private a persoanelor fizice; și, prin urmare, necesită o DPIA.
9. Atunci când prelucrarea în sine „*împiedică persoanele fizice să-și exercite un drept sau să utilizeze un serviciu sau un contract*" (art. 22 și Considerentul 91). 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.

În majoritatea cazurilor, un operator de date poate considera că o prelucrare ce îndeplinește 2 criterii ar necesita realizarea unei DPIA. În general, Grupul de Lucru Articolul 29 consideră că atunci când o prelucrare îndeplinește mai multe criterii, cu atât este mai probabil ca aceasta să prezinte un risc ridicat pentru drepturile și libertățile persoanelor vizate și, prin urmare, să impună efectuarea unei DPIA, indiferent de măsurile pe care operatorul le are în vedere să le adopte.

Totuși, în anumite situații, **un operator poate considera că prelucrarea care îndeplinește un singur criterii necesită efectuarea unei DPIA.**

Următoarele exemple ilustrează modul în care criteriile trebuie folosite pentru a analiza dacă o anumiă operațiune de prelucrare necesită o DPIA:

Exemple de prelucrare	Posibile criterii relevante	Este posibil ca DPIA să fie necesară?

Un spital prelucrează datele genetice și datele de sănătate ale pacienților săi (sistemul de informații al spitalului).	- Date sensibile sau date de natură foarte personală. - Date privind persoanele fizice vulnerabile. - Date prelucrate pe scară largă.	DA
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.	
Colectarea de date de social media publice pentru generarea de profiluri	- Evaluare sau scoring. - Date prelucrate pe scară largă. - Potrivirea sau combinarea seturilor de date. - Date sensibile sau date de natură foarte personală.	
O instituție care creează o bază de date la nivel național privind creditele sau privind frauda.	- Evaluare sau scoring. - Decizie automată care produce efecte juridice sau similare semnificative. - Împiedică persoana vizată să-și exercite un drept sau să utilizeze un serviciu sau un contract. - Date sensibile sau date de natură foarte personală.	
Stocarea în scop de arhivare a datelor personale sensibile pseudonimizate privind persoanele vizate vulnerabile din proiectele de cercetare sau studii clinice.	- Date sensibile. - Date privind persoanele vizate vulnerabile. - Împiedică persoana vizată să-și exercite un drept sau să utilizeze un serviciu sau un contract.	

Prelucrarea „datelor personale 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 de natură foarte personală. - Date privind persoanele vizate vulnerabile.	NU
O revistă online care folosește o listă de corespondență pentru a trimite un abonament generic zilnic abonaților săi.	- Date prelucrare pe scară largă.	
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.	

Dimpotrivă, o operațiune de prelucrare poate corespunde cazurilor menționate mai sus și este încă considerată de către operator că nu este „susceptibilă de a genera un risc ridicat". În astfel de cazuri, operatorul trebuie să justifice și să documenteze motivele pentru care nu a realizat o DPIA și să includă/să înregistreze opiniile responsabilului pentru protecția datelor.

În plus, ca parte a principiului responsabilității, fiecare operator de date „*va păstra o evidență a activităților de prelucrare desfășurate sub responsabilitatea sa*" ce va cuprinde, printre altele, scopurile prelucrării, o descriere a categoriilor de date și destinatarii datelor și „*acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la art. 32 (1)*" (art. 30 (1)) și trebuie să evalueze dacă există un risc ridicat, chiar dacă decid în cele din urmă să nu realizeze o DPIA.

Notă: autoritățile de supraveghere sunt obligate să stabilească, să publice și să comunice o listă a operațiunilor de prelucrare care necesită o DPIA către Comitetul European pentru Protecția Datelor (EDPB) (art. 35 (4))[18]. Criteriile menționate mai sus pot ajuta 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 datelor copiilor ar putea fi de asemenea considerată ca relevantă pentru elaborarea unei liste în conformitate cu art. 35 (4).

b) Când nu este obligatorie DPIA? Când prelucrarea nu este „susceptibilă să genereze un risc ridicat" sau când există DPIA similară sau când a fost autorizată anterior mai 2018 sau când există un temei legal sau când inclusă în lista operațiunilor de prelucrare pentru care DPIA nu este obligatorie

Grupul de Lucru Articolul 29 consideră că DPIA nu este necesară în următoarele situații:

- **atunci când prelucrarea nu este „*susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice*"** (art. 35 (1));
- **atunci când natura, obiectivul, contextul și scopurile prelucrării sunt foare similare prelucrării pentru care a fost realizată DPIA.** În astfel de situații, pot fi utilizate rezultatele DPIA pentru prelucrări similare (art. 35 (1)[19]);

[18] În acest context, „*autoritatea de supraveghere competentă aplică mecanismul pentrua asigurarea coerenței menționat la art. 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*" (art. 35 (6)).

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

- atunci când operațiunile de prelucrare au fost verificate de autoritatea de supraveghere înainte de mai 2018 în condiții specifice care nu au suferit modificări[20] (a se vedea III.C);
- **atunci când operațiunea de prelucrare**, potrivit literelor c) și e) de la art. 6 (1), **are un temei juridic** în dreptul Uniunii sau al unui stat membru, iar dreptul respectiv reglementează operațiunea de prelucrare **și deja s-a efectuat o DPIA** ca parte a unei evaluări a impactului generale în contextul adoptării respectivului temei juridic (art. 35 (10))[21], cu excepția cazului în care statul membru a declarat că este necesară efectuarea unei astfel de DPIA înaintea desfășurării activităților de prelucrare;
- **atunci când prelucrarea este inclusă pe lista opțională (stabilită de autoritatea de supraveghere) a operațiunilor de prelucrare** pentru care nu este necesară DPIA (art. 35 (5)). O astfel de listă poate conține activități de prelucrare care respectă condițiile specificate de această autoritate, în special prin ghiduri, decizii sau autorizații specifice, reguli de conformitate etc. (de exemplu, în Franța, autorizații, scutiri, reguli simplificate, pachete de conformitate...). În astfel de cazuri și sub rezerva reevaluării de către autoritatea de supraveghere competentă, o DPIA nu este necesară, ci numai dacă prelucrarea intră strict în sfera procedurii relevante menționate în listă și continuă să respecte pe deplin toate cerințele relevante din GDPR.

C. <u>Care este situația pentru operațiunile de prelucrare deja existente? DPIA este necesară în anumite situații</u>

Cerința de a realiza o DPIA se aplică operațiunilor de prelucrare existente care pot conduce la un risc ridicat pentru drepturile și libertățile persoanelor fizice și pentru care s-a produs o schimbare a riscurilor, luând în considerare natura, obiectivul, contextul și scopurile prelucrării.

DPIA nu este necesară pentru operațiunile de prelucrare ce au fost verificate de autoritatea de supraveghere sau de un funcționar în domeniul protecției datelor, în conformitate cu art. 20 din Directiva 95/46/CE și care sunt realizate într-un mod ce nu a suferit modificări 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, aceasta înseamnă că orice prelucrare a datelor ale cărei condiții de aplicare (domeniul de aplicare, scopul, datele personale colectate, identitatea operatorilor sau destinatarilor datelor, perioada de păstrare a datelor, măsurile tehnice și organizatorice etc.) s-au schimbat de la verificarea prealabilă efectuată de autoritatea de supraveghere sau funcționarul în materie de protecție a datelor și care ar putea genera un risc ridicat ar trebui să facă obiectul unei DPIA.

Mai mult, o DPIA ar putea fi necesară după o schimbare a riscurilor rezultate din operațiunile de prelucrare[22], de exemplu pentru că o nouă tehnologie a intrat în uz sau pentru că datele cu caracter personal sunt utilizate într-un alt scop. Operațiile de prelucrare a datelor pot evolua rapid și pot apărea noi

[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 realizează în etapa de elaborare a legislației care furnizează un temei juridic pentru o prelucrare, este probabil să fie nevoie de o revizuire înainte de începerea operațiunilor, deoarece legislația adoptată poate fi diferită față de propunere în sensul în care afectează viața privată și protecția datelor. În plus, este posibil să nu existe suficiente detalii tehnice privind prelucrarea efectivă în momentul adoptării legislației, chiar dacă aceasta este însoțită de o DPIA. În astfel de cazuri, poate fi necesar să se efectueze o DPIA specifică înainte de efectuarea activităților de prelucrare efectivă.

[22] În ceea ce privește contextu, datele colectate, scopurile, funcționalitățile, datele cu caracter personal prelucrate, destinatarii, combinările de date, riscuri (activele de suport, sursele riscurilor, impactul potențial, amenințări etc.), măsurile de securitate și transferurile internaționale.

vulnerabilități. Prin urmare, trebuie remarcat faptul că revizuirea unei DPIA nu este utilă numai pentru îmbunătățirea continuă, dar este, de asemenea, esențială pentru menținerea nivelului de protecție a datelor într-un mediu în schimbare în timp. O DPIA poate deveni, de asemenea, necesară deoarece contextul organizațional sau societal pentru activitatea de prelucrare s-a schimbat, de exemplu, deoarece efectele anumitor decizii automate au devenit mai semnificative sau noile categorii de persoane vizate devin vulnerabile la discriminare. Fiecare dintre aceste exemple ar putea constitui un element care să conducă la o schimbare a riscului care rezultă din activitatea de prelucrare în cauză.

Dimpotrivă, anumite schimbări ar putea reduce riscul. De exemplu, o operațiune de prelucrare ar putea evolua astfel încât deciziile să nu mai fie automate sau dacă o activitate de monitorizare nu mai este sistematică. În acest caz, revizuirea analizei de risc realizate poate arăta că efectuarea unei DPIA nu mai este necesară.

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

D. Cum se realizează DPIA?

a) În ce moment trebuie efectuată DPIA? Anterior prelucrării

DPIA trebuie realizată „anterior prelucrării" (art. 35 (1) și art. 35 (1), Considerentele 90 și 93)[23]. Acest asptect este în concordanță cu asigurarea protecției datelor începând cu momentul conceperii și în mod implicit (art. 25 și Considerentul 78). DPIA ar trebui văzută ca un instrument pentru a ajuta la luarea deciziilor cu privire la prelucrare.

DPIA ar trebui să înceapă cât mai curând posibil întrucât este practică în stadiul proiectării operațiunii de prelucrare, chiar dacă unele dintre operațiile de prelucrare sunt încă necunoscute. Actualizarea DPIA pe parcursul întregului ciclu de viață va asigura luarea în considerare a protecției datelor și a vieții private și va încuraja crearea de soluții care să promoveze respectarea normelor. De asemenea, poate fi necesară repetarea etapelor individuale ale evaluării pe măsură ce procesul de dezvoltare progresează, deoarece selectarea anumitor măsuri tehnice sau organizatorice poate afecta severitatea sau probabilitatea riscurilor generate de prelucrare.

Faptul că DPIA ar trebui să fie actualizată odată ce procesul de prelucrare a început efectiv nu este un motiv valid pentru amânarea sau neaplicarea unei DPIA. DPIA este un proces în desfășurare, în special în cazul în care o operațiune de prelucrare este dinamică și este supusă unor schimbări continue. **Efectuarea unei DPIA este un proces continuu, nu un exercițiu unic.**

b) Cine are obligația să efectueze DPIA? Operatorul, împreună cu DPO și împuterniciți

Operatorul este responsabil pentru realizarea unei DPIA (art. 35 (2)). DPIA poate fi realizată și de altcineva din interiorul sau exteriorul organizației, dar operatorul rămâne în cele din urmă responsabil pentru această sarcină.

[23] Cu excepția cazului în care o prelucrare deja existentă care a fost verificată anterior de autoritatea de supraveghere, caz în care DPIA ar trebui să fie efectuată înainte de a fi supuse unor modificări semnificative.

De asemenea, operatorul trebuie să solicite avizul responsabilului cu protecția datelor (DPO), în cazul în care acesta este desemnat (art. 35 (2)) și acest aviz, precum și deciziile luate de operator, ar trebui să fie documentate în cadrul DPIA. De asemenea, DPO ar trebui să monitorizeze funcționarea DPIA (art. 39 (1) litera (c)). Ghidul Grupului de Lucru Articolul 29 privind responsabilul cu protecția datelor 16/EN WP 243 oferă instrucțiuni suplimentare.

Dacă prelucrarea este efectuată parțial sau în totalitate de persoana împuternicită de operator, **persoana împuternicită de operator va ajuta operatorul la realizarea DPIA** și va oferi informațiile necesare (în conformitate cu art. 28 (3) litera f)).

Operatorul trebuie „*să solicite avizul persoanelor vizate sau al reprezentanților acestora*" (art. 35 (9)), „*acolo unde este cazul*". Grupul de Lucru Articolul 29 consideră că:

- aceste opinii ar putea fi solicitate printr-o varietate de mijloace, în funcție de context (de exemplu, un studiu generic referitor la scopul și mijloacele operațiunii de prelucrare, o întrebare adresată reprezentanților personalului sau sondajele obișnuite transmise viitorilor clienți ai operatorului de date) asigurându-se că operatorul are o bază legală pentru prelucrarea datelor personale implicate în căutarea unor astfel de opinii. Deși trebuie menționat faptul că acordul de prelucrare nu este în mod evident o modalitate de a căuta opiniile persoanelor vizate;
- în cazul în care decizia finală a operatorului de date diferă de opiniile persoanelor vizate, motivele continuării sau nu ar trebui documentate;
- operatorul ar trebui, de asemenea, să documenteze justificarea că nu a solicitat opiniile persoanelor vizate, în cazul în care decide că acest lucru nu este adecvat, de exemplu dacă acest lucru ar compromite confidențialitatea planurilor de afaceri ale societăților sau ar fi disproporționat sau imposibil de realizat.

Pe final, definirea și documentarea altor roluri și responsabilități specifice, în funcție de politica, procesele și regulile interne este o bună practică, de exemplu:

- atunci când unitățile de afaceri specifice pot propune efectuarea unei DPIA, respectivele unități ar trebui să furnizeze date pentru DPIA și ar trebui să fie implicate în procesul de validare al DPIA;
- se recomandă solicitarea avizului din partea experților independenți din diferite profesii[24] (avocați, experți IT, experți în securitate, sociologi, etică etc.), dacă este cazul;
- trebuie definite în mod contractual rolurile și responsabilitățile persoanelor împuternicite de operator; iar DPIA trebuie să fie efectuată cu ajutorul persoanei împuternicite de operator, ținând seama de natura prelucrării și de informațiile disponibile pentru persoana împuternicită de operator (art. 28 (3) f));
- responsabilul șef cu securitatea informațiilor (Chief Information Security Officer), dacă este desemnat, precum și DPO, ar putea sugera că operatorul să efectueaze o DPIA pe o anumită operațiune de prelucrare și ar trebui să ajute părțile interesat cu privire la metodologie, să contribuie la evaluarea calității evaluării riscului și dacă riscul rezidual este acceptabil și să dezvolte cunoștințe specifice contextului operatorului de date;
- responsabilul șef cu securitatea informațiilor (Chief Information Security Officer), dacă este numit, și/sau departamentul IT, ar trebui să ofere asistență operatorului și ar putea propune efectuarea unei DPIA pentru o anumită operațiune de prelucrare, în funcție de cerințele de securitate sau operaționale..

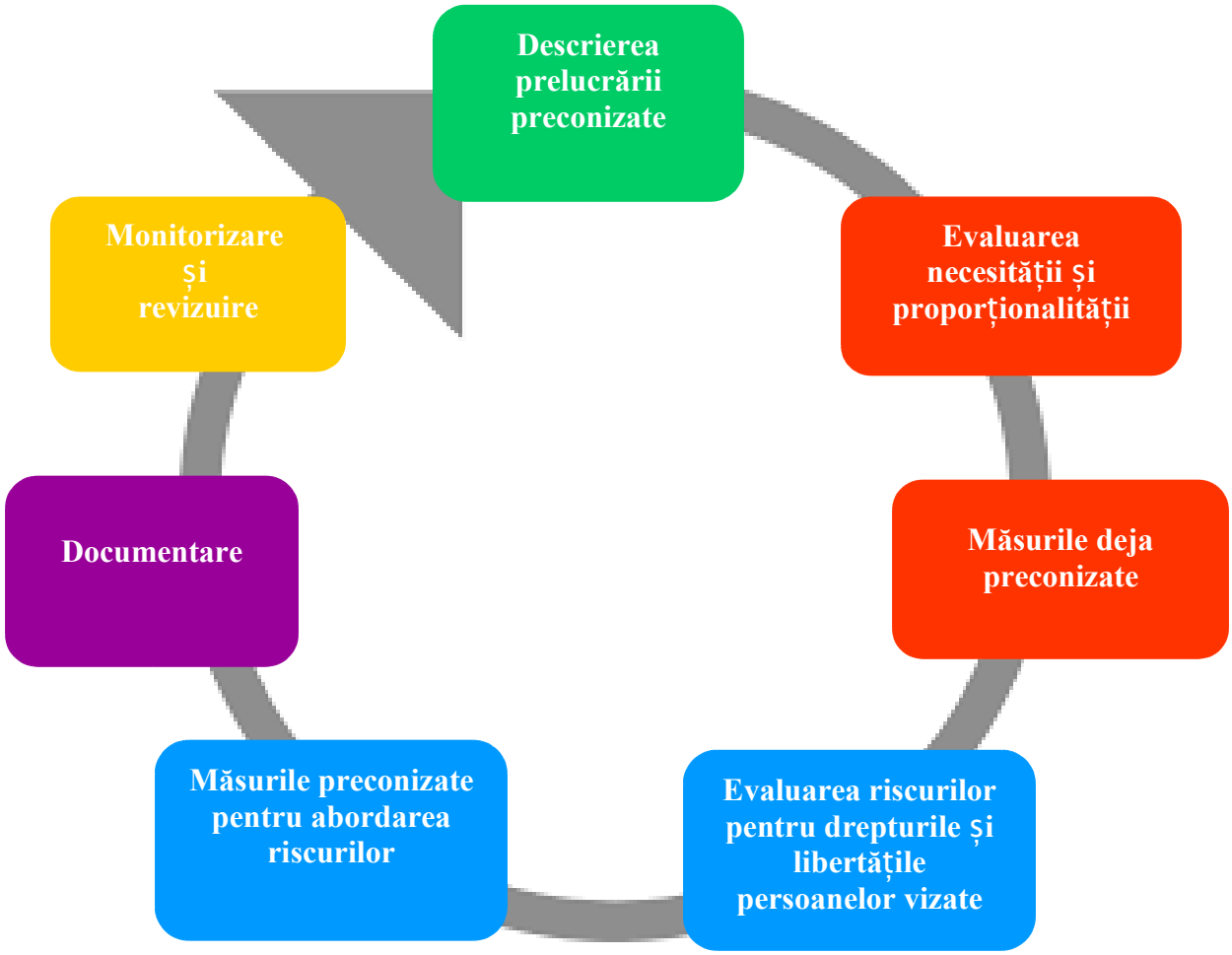
c) Care este metodologia pentru efectuarea DPIA? Metodologii diferite, dar criterii comune

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

RGPD stabilește caracteristicile minime ale unei DPIA (art. 35 (7) și Considerentele 84 și 90):

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

Figura următoare ilustrează procesul generic iterativ pentru realizarea unei DPIA[25]:



Trebuie avută în vedere respectarea (art 35 (8)) unui cod de conduită (art. 40) atunci când se evaluează impactul unei operațiuni de prelucrare a datelor. Acest lucru poate fi util pentru a demonstra că au fost alese sau introduse măsuri adecvate, cu condiția ca respectivul cod de conduită să fie adecvat operațiunii de prelucrare. Trebuie avute în vedere și certificările, sigiliile și mărci (art. 42), precum și Regulile corporatiste obligatorii (BCR) în scopul demonstrării conformității cu RGPD a operațiunilor de prelucrare efectuate de operatori și persoane împuternicite de operatori.

[25] Trebuie subliniat faptul că procesul descris aici este iterativ: în practică, este probabil ca fiecare dintre etape să fie revizuită de mai multe ori înainte ca DPIA să poate fi finalizată.

Toate cerințele relevante stabilite în RGPD oferă un cadru larg, generic pentru proiectarea și realizarea unei DPIA. Implementarea practică a unei DPIA va depinde de cerințele stabilite în RGPD care pot fi completate cu orientări practice mai detaliate. Prin urmare, implementarea DPIA este scalabilă. Acest lucru înseamnă că și un operator de date mic poate proiecta și implementa o DPIA care este potrivită pentru operațiunile de prelucrare a acestuia.

Considerentul 90 al RGPD conturează o serie de componente ale DPIA care se suprapun cu componente bine definite ale managementului riscului (de exemplu, ISO 31000[26]). În ceea ce privește managementul riscurilor, DPIA vizează „gestionarea riscurilor" asupra drepturilor și libertăților persoanelor fizice, utilizând următoarele procese, prin:

- stabilirea contextul: „*ținând cont de natura, obiectivul, contextul și scopurile prelucrării și sursele riscului*";
- evaluarea riscurilor: „*evaluarea probabilității și gravității deosebite a riscului ridicat*";
- tratarea riscurilor: „*atenuarea acestui risc*" și „*asigurarea protecției datelor cu caracter personal*" și „*demonstrarea conformității cu dispozițiile prezentului Regulament*".

Notă: DPIA potrivit RGPD reprezintă un instrument de gestionare a riscurilor pentru drepturile persoanelor vizate și, prin urmare, prezintă perspectiva acestora, ca în anumite domenii (de exemplu, securitatea societății). În schimb, gestionarea riscurilor în alte domenii (de exemplu, securitatea informațiilor) se concentrează asupra organizației.

RGPD oferă operatorilor de date flexibilitatea de a determina structura și forma exactă a DPIA, pentru a permite ca aceasta să se potrivească practicilor de lucru existente. Există un număr de procese diferite stabilite în UE și în întreaga lume care iau în considerare componentele descrise în Considerentul 90. Cu toate acestea, indiferent de forma sa, DPIA trebuie să fie o evaluare reală a riscurilor, permițând operatorilor adoptarea de măsuri în vederea atenuării acestora.

Ar putea fi utilizate metodologii diferite (a se vedea Anexa 1 pentru exemple de metodologii de evaluare a impactului asupra protecției datelor și a vieții private) pentru a contribui la punerea în aplicare a cerințelor de bază stabilite în RGPD. Au fost identificate criterii comune pentru a permite existența unor astfel de abordări diferite și, în același timp, pentru a permite operatorilor să respecte RGPD (a se vedea anexa 2). Respectivele criterii clarifică cerințele de bază ale Regulamentului și oferă suficiente posibilități pentru diferite forme de punere în aplicare. Aceste criterii pot fi folosite pentru a arăta că o anumită metodologie DPIA îndeplinește standardele cerute de RGPD. **Depinde de operatorul de date să aleagă o metodologie, însă această metodologie ar trebui să fie conformă cu criteriile prevăzute în Anexa 2**.

Grupul de Lucru Articolul 29 încurajează dezvoltarea cadrelor DPIA specifice sectoarelor. Acest lucru se datorează faptului că acestea se pot baza pe cunoștințe sectoriale specifice, ceea ce înseamnă că DPIA poate aborda specificul unui anumit tip de operațiune de prelucrare (de exemplu: tipuri specifice de date, active corporative, impacturi potențiale, amenințări, măsuri). Aceasta înseamnă că DPIA poate aborda problemele care apar într-un anumit sector economic sau când se utilizează tehnologii particulare sau care desfășoară anumite tipuri de operațiuni de prelucrare.

Pe final, atunci când este necesar, „*operatorul efectuează o analiză pentru a evaluarea 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*" (art. 35 (11)[27])

[26] Procesele de management al riscului: comunicare și consultare, stabilirea contextului, evaluarea riscurilor, tratarea riscurilor, monitorizarea și revizuirea (a se vedea termenii și definițiile și cuprinsul din ISO 31000 previzualizare: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

[27] Art. 35(10) exclude în mod explicit numai aplicarea art. 35 (1) – (7).

d) Există vreo obligație de a publica DPIA? Nu, dar publicarea unui rezumat poate oferi încredere, iar DPIA integrală poate fi comunicată autorității de supraveghere în cazul unei consultări prealabile sau la solicitarea DPA

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

Scopul unui astfel de proces ar fi să contribuie la încurajarea încrederii în operațiunile de prelucrare ale operatorului și să demonstreze responsabilitatea și transparența. Este o practică deosebit de bună de a publica o DPIA atunci când membrii publicului sunt afectați de operațiunea de prelucrare. Acest lucru ar putea fi, în special, cazul în care o autoritate publică efectuează o DPIA.

DPIA publicată nu trebuie să conțină întreaga evaluare, mai ales atunci când DPIA ar putea să prezinte informații specifice privind riscurile de securitate pentru operatorul de date sau să dezvăluie secrete comerciale sau informații comerciale sensibile. În aceste condiții, versiunea publicată ar putea constitui doar un rezumat al principalelor constatări ale DPIA sau chiar doar o afirmație potrivit căreia a fost efectuată o DPIA.

Mai mult, în cazul în care o DPIA dezvăluie riscuri reziduale ridicate, operatorul de date va trebui să solicite consultări prealabile pentru prelucrarea de la autoritatea de supraveghere (art. 36 (1)). Ca parte a acestui fapt, DPIA trebuie să fie furnizată complet (articolul 36 (3) (e)). Autoritatea de supraveghere poate să furnizeze opinia sa[28] și nu va compromite secretele comerciale sau nu va dezvălui vulnerabilitățile privind securitatea, sub rezerva principiilor aplicabile în fiecare stat membru privind accesul public la documentele oficiale.

E. Când trebuie consultată autoritatea de supraveghere? Când riscurile residuale sunt ridicate

Așa cum a fost explicat mai sus:

- o DPIA este necesară atunci când o operațiunie de prelucrare „*este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice*" (art. 35 (1), a se vedea III.B.a). Ca exemplu, prelucrarea pe scară largă a datelor privind starea de sănătate este considerată ca fiind susceptibilă să genereze un risc ridicat și necesită o DPIA;
- atunci este responsabilitatea operatorului de date să evalueze riscurile pentru drepturile și libertățile persoanelor vizate și să identifice măsurile[29] prevăzute pentru a reduce aceste riscuri la un nivel acceptabil și pentru a demonstra conformitatea cu RGPD (art. 35 (7), a se vedea III.C.c). Un exemplu ar putea fi utilizarea unor măsuri de securitate tehnice și organizaționale adecvate (criptarea eficientă a discului complet, gestionarea robustă a cheilor, controlul adecvat al accesului, copiile securizate etc.) pe lângă politicile existente (notificarea, consimțământul, dreptul de acces, dreptul de a se opune etc.) pentru stocarea datelor cu caracter personal pe computerele portabile.

În exemplul computerului portabili de mai sus, în cazul în care riscurile au fost considerate suficient de reduse de către operatorul de date și în urma citirii art. 36 (1) și a Considerentelor 84 și 94, prelucrarea poate continua fără consultarea autorității de supraveghere. În cazurile în care riscurile identificate nu pot

[28] Consultarea scrisă a operatorului este necesară numai atunci când autoritatea de supraveghere consideră că prelucrarea intenționată nu este conformă cu regulamentul așa cum este prevăzut la art. 36(2).

[29] Inclusiv luarea în considerare orientările existente ale EDPB și ale autorităților de supraveghere, ținând cont de stadiuil tehnicii și costurile de punere în aplicare, în conformitate cu art. 35 (1).

fi abordate suficient de către operatorul de date (adică riscurile reziduale rămân ridicate), operatorul de date trebuie să consulte autoritatea de supraveghere.

Un exemplu de risc rezidual ridicat inacceptabil include cazurile în care persoanele vizate pot întâmpina consecințe semnificative sau chiar ireversibile pe care nu le pot depăși (de exemplu: accesul ilegal la datele care duc la amenințarea vieții persoanelor vizate, concediere, risc financiar) și/sau când pare evident că riscul va avea loc (de exemplu: prin faptul că nu este capabil să reducă numărul de persoane care accesează datele datorită modalităților de partajare, de utilizare sau distribuție sau atunci când vulnerabilitatea bine cunoscut nu este înlăturată).

Este necesară consultarea cu autoritatea de supraveghere[30] de fiecare dată când operatorul de date nu poate găsi suficiente măsuri pentru a reduce riscurile la un nivel acceptabil (adică riscurile reziduale sunt încă ridicate).

În plus, operatorul va trevui să consulte autoritatea de supraveghere atunci dreptul intern impune operatorilor să consulte autoritatea de supraveghere și/sau să obțină autorizarea prealabilă din partea acesteia în ceea ce privește prelucrarea de către un operator pentru îndeplinirea unei sarcini exercitate de operator în interes public, inclusiv prelucrarea în legătură cu protecția socială și sănătatea publică (art. 36 (5)).

Cu toate acestea, trebuie precizat faptul că obligațiile de a păstra o evidență a DPIA și de a actualiza DPIA în timp util rămân, indiferent dacă este necesară sau nu consultarea autorității de supraveghere în funcție de nivelul riscului rezidual.

IV. CONCLUZII ȘI RECOMANDĂRI

DPIA reprezintă o modalitate utilă pentru operatorii de date de a implementa sisteme de prelucrare a datelor care respectă RGPD și pot fi obligatorii pentru anumite tipuri de operațiuni de prelucrare. Acestea sunt scalabile și pot lua forme diferite, dar RGPD stabilește cerințele de bază ale unei DPIA eficiente. Operatorii de date ar trebui să considere că realizarea unei DPIA reprezintă o activitate utilă și pozitivă care ajută la respectarea legislației.

Art. 24 (1) stabilește responsabilitatea de bază pentru operatorii de date în ceea ce privește respectarea RGPD: „*ținând 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, opeartorul 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 o parte esențială a respectării Regulamentului atunci când este planificată sau are loc o prelucrare a datelor cu risc ridicat. Aceasta înseamnă că operatorii de date ar trebui să utilizeze criteriile stabilite în acest document pentru a stabili dacă trebuie sau nu să realizeze o DPIA. Politica internă a operatorului de date ar putea extinde această listă în afara cerințelor legale ale RGPD. Acest lucru ar trebui să ducă la o mai mare încredere a persoanelor vizate și a altor operatori de date.

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

[30] Notă: „*pseudonimizarea sau criptarea datelor cu caracter personal*” (precum și minimizarea, mecanismul de supraveghere etc.) nu sunt neapărat măsuri corespunzătoare. Sunt doar exemple. Măsurile corespunzătoare depinde context și riscuri, specifice operațiunilor de prelucrare.

- să aleagă o metodologie DPIA (exemple prezentate în Anexa 1) care să îndeplinească creiteriile din Anexa 2 sau să specifice și să implementexe un proces sistematic de DPIA care:
    - să fie în conformitate cu criteriile din Anexa 2;
    - este integrat în procesele existente de proiectare, dezvoltare, schimbare, risc și revizuire operațională, în conformitate cu procedurile interne, contextul și cultura;
    - implică părțile interesată și care definește în mod clar responsabilitățile acestora (operatorul, DPO, persoanele vizate sau reprezentanții acestora, întreprinderi, servicii tehnice, persoanele împuternicite de operatori, ofițerii de securitate a informațiilor etc.);
- să furnizeze raportul DPIA autorității de supraveghere competente atunci când este necesar să o facă;
- să consulte autoritatea de supraveghere atunci când nu a reușit să stabilească suficiente măsuri pentru atenuarea riscurilor ridicate;
- să revizuiască periodic DPIA și procesele pe care le evaluează, cel puțin atunci când există o schimbare a riscului reprezentat de prelucrarea operațiuinii;
- să documenteze deciziile luate.

ANEXA 1 – EXEMPLE DE DPIA EXISTENTE LA NIVELUL UE

RGPD nu specifică ce procedură DPIA trebuie urmată, ci permite operatorilor de date să introducă un cadru care să completeze practicile lor de lucru existente, cu condiția să ia în considerare componentele descrise la art. 35 (7). Un astfel de cadru poate fi personalizat pentru operatorul de date sau poate fi comun într-o anumită industrie. Cadrele publicate anterior, elaborate de DPA-urile UE și cadrele specifice sectorului UE, includ (dar nu se limitează la acestea):

Exemple de cadre generice UE:

- DE: Standard Data Protection Model, V.1.0 – Trial version, 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.

[31] În mod unanim și afirmativ recunoscut (cu excepția Bavariei) de către cea de-a 92a Conferință a Autorităților Independente pentru Protecția datelor la nivel Federal și la nivelul Land-urilor, Kühlungsborn, în perioada 9-10 noiembrie 2016.

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

- FR: *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
  https://www.cnil.fr/fr/node/15798
- UK: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014.
  https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Exemple de cadre specifice sectorului UE:

- Cadru de evaluare a impactului asupra protecției datelor și vieții private a aplicațiilor RFID[32].
- Scenariul de evaluare a impactului asupra protecția datelor pentru sistemele inteligente de rețea și de măsurare inteligentă[33].

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

ANEXA 2 – CRITERII PENTRU O DPIA ACCEPTATĂ

Grupul de Lucru Articolul 29 propune următoarele criterii pe care operatorii de date le pot utiliza pentru a evalua dacă o DPIA sau o metodologie de realizare a unei DPIA este suficient de cuprinzătoare pentru a se conforma RGPD:

- se furnizează o descriere sistematică a prelucrării (art. 35 (7) a)):
  - se ține cont de natura, domeniul de aplicare, contextul și scopurile prelucrării (Considerentul 90);
  - se înregistrează datele cu caracter personal, destinatarii, și perioada pentru care datele cu caracter personal sunt stocate;
  - se furnizează o descriere funcțională a operațiunii de prelucrare;
  - se identifică activele pe care se bazează datele cu caracter personal (hardware, software, rețelele, persoanele, documentele pe suport hârtie sau canalele de transmitere pe suport de hârtie);
  - se ține cont de respectarea codurilor de conduită aprobate (art. 35 (8));
- se evaluează necesitatea și proporționalitatea (art. 35 (7) b)):
  - se determină măsurile preconizate în vederea conformării cu Regulamentul (art. 35 (7) d) și Considerentul 90), având în vedere:

[32] A se vedea de asemenea:
- Recomandarea Comisiei din 12 mai 2009 privind implementarea principiilor de viață privată și protecția datelor în aplicațiile suportate de identificarea prin radio-frecvență.
  https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- Opinia 9/2011 privind propunerea revizuită a sectorului industrial referitoare la un cadru de evaluare a impactului aplicațiilor RFID asupra vieții private și a datelor.
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_en.pdf

[33] A se vedea de asemenea Opinia 07/2013 prividn scenariul de evaluare a impactului asupra protecției datelor pentru sistemele inteligente de rețea și de măsurare inteligentă („Model DPIA"), elaborată de Grupul de Experți 2 pentru Grupului Task Force al Comisiei privind sistemele inteligente.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf

[34] ISO/IEC 29134 (proiect), *Tehnologia informației – Tehnici de securitate – Evaluare de impact asupra vieții private – Ghid*, Organizația Internațională de Standardizare (ISO).

        - măsuri care contribuie la proporționalitatea și necesitatea prelucrării pe baza:
            - scopurilor determinate, explicite și legitime (art. 5 (1) b));
            - legalitatea prelucrării (art. 6);
            - adecvate, relevante și limitate la ceea ce este necesar (art. 5 (1) c));
            - perioadă de stocare limitată (art. 5 (1) e));
        - măsuri care contribuie la drepturile persoanelor vizate:
            - informațiile furnizate persoanei vizate (art. 12, 13 și 14);
            - dreptul de acces și dreptul la portabilitatea datelor (art. 15 și 20);
            - dreptul la rectificare și dreptul la ștergere (art. 16, 17 și 19);
            - dreptul la opoziție și dreptul la restricționarea prelucrării (art. 18, 19 și 21);
            - relațiile cu persoanele împuternicite de operator (art. 28);
            - garanțiile pentru transferurile internaționale (Capitolul V);
            - consultarea prealabilă (art. 36).
- se gestionează riscurile pentru drepturile și libertățile persoanelor vizate (art. 35 (7) c)):
    - se analizează originea, natura, particularitatea și gravitatea riscurilor (a se vedea Considerentul 84) sau, mai exact, pentru fiecare risc (acces ilegal, modificări nedorite și dispariția datelor) din perspectiva persoanelor vizate:
        - se ține cont de sursele riscurilor (Considerentul 90);
        - se identifică impactul posibil asupra drepturilor și libertăților persoanelor vizate în cazul unor evenimente ce includ accesul ilegal, modificările nedorite sau dispariția datelor;
        - se identifică amenințările care ar putea conduce la accesul ilegal, modificarea nedorită sau dispariția datelor;
        - se estimează probabilitatea și gravitatea (Considerentul 90);
    - se determină măsurile preconizate pentru atenuarea respectivelor riscuri (art. 35 (7) d) și Considerentul 90);
- sunt implicate părțile interesate:
    - se solicită avizul DPO (art. 35 (2));
    - se solicită, acolo unde este cazul, avizul peroanelor vizate sau al reprezentanților acestora (art. 35 (9)).