
# Orientările nr. 4/2019 privind articolul 25

# Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit

## Versiunea 2.0

## Adoptate la 20 octombrie 2020

## Istoric versiuni

| | | |
|---|---|---|
| Versiunea 1.0 | 13 noiembrie 2019 | Adoptarea orientărilor pentru consultare publică |
| Versiunea 2.0 | 20 octombrie 2020 | Adoptarea orientărilor de către CEPD în urma consultării publice |

## Cuprins

## Comitetul european pentru protecția datelor,

având în vedere articolul 70 alineatul (1) litera (e) din Regulamentul 2016/679/UE 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 (denumit în continuare „RGPD”),

având în vedere Acordul privind SEE, în special anexa XI și Protocolul 37 la acesta, astfel cum au fost modificate prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018,

având în vedere articolul 12 și articolul 22 din Regulamentul său de procedură,

**ADOPTĂ URMĂTOARELE ORIENTĂRI:**


**Rezumat**

Într-o lume din ce în ce mai digitalizată, respectarea cerințelor privind asigurarea protecției datelor începând cu momentul conceperii și în mod implicit joacă un rol esențial în promovarea confidențialității și a protecției datelor în societate. Prin urmare, este esențial ca operatorii să trateze această răspundere cu seriozitate și să pună în aplicare obligațiile RGPD atunci când concep operațiunile de prelucrare.

Prezentele orientări oferă îndrumări generale cu privire la obligația de asigurare a protecției datelor începând cu momentul conceperii și în mod implicit (denumită în continuare „DPbDD”), astfel cum se prevede la articolul 25 din RGPD. DPbDD este o obligație aplicabilă tuturor operatorilor, indiferent de dimensiunea acestora și de complexitatea variabilă a prelucrării. Pentru a putea pune în aplicare cerințele DPbDD, este esențial ca operatorul să înțeleagă principiile de protecție a datelor, precum și drepturile și libertățile persoanei vizate.

Obligația fundamentală constă în punerea în aplicare a măsurilor *adecvate* și a garanțiilor necesare care să asigure *respectarea efectivă* a *principiilor de protecție a datelor* și, prin urmare, a *drepturilor și libertăților persoanelor vizate începând cu momentul conceperii și în mod implicit*. Articolul 25 stabilește atât elementele legate de concepere, cât și de protecția implicită care trebuie luate în considerare. Elementele respective vor fi aprofundate în cadrul acestor orientări.

Articolul 25 alineatul (1) stipulează că, atunci când planifică o nouă operațiune de prelucrare, operatorii trebuie să ia în considerare DPbDD într-o fază incipientă. Operatorii trebuie să pună în aplicare DPbDD *înainte* de prelucrare și *în permanență* la momentul prelucrării, revizuind regulat eficacitatea măsurilor și a garanțiilor selectate. DPbDD se aplică și sistemelor existente care prelucrează date cu caracter personal.

Orientările conțin, de asemenea, îndrumări privind modul în care pot fi puse în aplicare în mod eficace principiile de protecție a datelor prevăzute la articolul 5, prezentând principalele elemente legate de protecția implicită și din momentul conceperii, precum și situații practice cu scop ilustrativ. Operatorul trebuie să aibă în vedere adecvarea măsurilor sugerate în contextul prelucrării specifice în cauză.

CEPD oferă recomandări cu privire la modul în care operatorii, persoanele împuternicite de operatori și producătorii pot coopera pentru a asigura DPbDD. Comitetul încurajează operatorii din domeniu, persoanele împuternicite de operatori și producătorii să utilizeze DPbDD ca mijloc de obținere a unui avantaj competitiv atunci când își comercializează produsele către operatori și către persoanele vizate. De asemenea, încurajează toți operatorii să utilizeze certificări și coduri de conduită.

# 1 DOMENIUL DE APLICARE

1. Orientările se concentrează asupra punerii în aplicare a DPbDD, în baza obligației prevăzute articolul 25 din RGPD.[1] Alți actori, de exemplu persoanele împuternicite de operatori și producătorii de produse, servicii și aplicații (denumiți în continuare „producătorii"), care nu sunt vizați în mod direct de articolul 25, pot să constate de asemenea că prezentele orientări sunt utile în crearea unor produse și servicii care respectă RGPD și ajută operatorii să-și îndeplinească obligațiile privind protecția datelor.[2] Considerentul 78 din RGPD adaugă că principiile DPbDD ar trebui să fie luate în considerare și în contextul licitațiilor publice. În pofida faptului că toți operatorii au datoria de a integra DPbDD în activitățile lor de prelucrare, această dispoziție încurajează adoptarea principiilor de protecție a datelor, iar în acest sens administrațiile publice ar trebui să conducă prin puterea exemplului. Operatorul răspunde de respectarea obligațiilor DPbDD în contextul prelucrării efectuate de persoanele împuternicite de operator și de subcontractanții acestora din urmă, iar acest lucru trebuie avut în vedere la contractarea părților respective.

2. Cerința descrisă la articolul 25 prevede ca operatorii să țină cont de conceptul de protecție a datelor ca setare implicită în prelucrarea datelor cu caracter personal, obligație care se aplică pe parcursul întregului ciclu de prelucrare. DPbDD este o cerință și pentru sistemele de prelucrare existente înaintea intrării în vigoare a RGPD. Operatorii trebuie să își actualizeze constant modul de prelucrare în conformitate cu RGPD. Pentru mai multe informații privind modul de menținere a unui sistem existent în conformitate cu DPbDD, a se vedea subcapitolul 2.1.4 din aceste orientări. Esența dispoziției constă în asigurarea unei protecții *adecvate* și *eficace* a datelor atât *începând cu momentul conceperii*, cât și *în mod implicit*, ceea ce înseamnă că operatorii trebuie să poată demonstra că au pus în aplicare în cadrul prelucrării măsuri și garanții adecvate pentru a asigura respectarea deplină a principiilor de protecție a datelor și a drepturilor și libertăților persoanelor vizate.

3. Capitolul 2 al orientărilor se concentrează asupra unei interpretări a cerințelor stabilite la articolul 25 și analizează obligațiile legale introduse de dispoziție. În capitolul 3 se prezintă exemple privind modul de aplicare a DPbDD în contextul principiilor specifice de protecție a datelor.

4. În capitolul 4, orientările abordează posibilitatea de a institui un mecanism de certificare pentru a demonstra respectarea articolului 25, iar în capitolul 5 – modul în care articolul poate fi pus în aplicare de autoritățile de supraveghere. La final, orientările le oferă părților interesate recomandări

[1] Interpretările oferite în prezentul document se aplică în aceeași măsură articolului 20 din Directiva (UE) 2016/680 și articolului 27 din Regulamentul (UE) 2018/1725.

[2] Considerentul 78 din RGPD stabilește în mod clar această necesitate: *„Atunci când elaborează, proiectează, selectează și utilizează aplicații, servicii și produse care se bazează pe prelucrarea datelor cu caracter personal sau care prelucrează date cu caracter personal pentru a-și îndeplini rolul, producătorii acestor produse și furnizorii acestor servicii și aplicații ar trebui să fie încurajați să aibă în vedere dreptul la protecția datelor la momentul elaborării și proiectării unor astfel de produse, servicii și aplicații și, ținând cont de stadiul actual al dezvoltării, să se asigure că operatorii și persoanele împuternicite de operatori sunt în măsură să își îndeplinească obligațiile referitoare la protecția datelor."*

suplimentare privind modul în care pot pune în aplicare cu succes DPbDD. Pentru a respecta pe deplin obligațiile legate de DPbDD, CEPD recunoaște provocările cu care se confruntă întreprinderile mici și mijlocii (denumite în continuare „IMM-uri”) și oferă recomandări suplimentare adresate specific IMM-urilor în capitolul 6.

# 2 ANALIZA ARTICOLULUI 25 ALINEATELE (1) ȘI (2): ASIGURAREA PROTECȚIEI DATELOR ÎNCEPÂND CU MOMENTUL CONCEPERII ȘI ÎN MOD IMPLICIT

5. Scopul prezentului capitol este de a analiza și de a oferi orientări privind cerința referitoare la protecția datelor începând cu momentul conceperii, prevăzută la articolul 25 alineatul (1) și, respectiv, cerința referitoare la protecția datelor în mod implicit, prevăzută la articolul 25 alineatul (2). Protecția datelor începând cu momentul conceperii și protecția datelor în mod implicit sunt concepte complementare, care se potențează reciproc. Persoanele vizate beneficiază într-o măsură mai mare de protecția implicită a datelor dacă în paralel se aplică și protecția începând cu momentul conceperii – și viceversa.

6. DPbDD este o cerință aplicabilă în egală măsură tuturor operatorilor, inclusiv întreprinderilor mici și companiilor multinaționale. Acestea fiind spuse, nivelul de complexitate asociat punerii în aplicare a DPbDD poate varia în funcție de fiecare operațiune de prelucrare în parte. În toate cazurile însă, indiferent de dimensiune, punerea în aplicare a DPbDD este benefică atât pentru operator, cât și pentru persoana vizată.

## 2.1 Articolul 25 alineatul (1): protecția datelor începând cu momentul conceperii

### 2.1.1 Obligația operatorului de a pune în aplicare măsuri tehnice și organizatorice adecvate și garanțiile necesare în cadrul prelucrării

7. În conformitate cu articolul 25 alineatul (1), operatorul trebuie să pună în aplicare *măsuri* tehnice și organizatorice *adecvate*, destinate să pună în aplicare principiile de protecție a datelor și să integreze *garanțiile necesare* în cadrul prelucrării, pentru a îndeplini cerințele și a proteja drepturile și libertățile persoanelor vizate. Atât măsurile adecvate, cât și garanțiile necesare au rolul de a deservi același scop de a proteja drepturile persoanelor vizate și de a asigura integrarea protecției datelor cu caracter personal ale acestora în cadrul prelucrării.

8. *Măsurile tehnice și organizatorice* și *garanțiile* necesare pot fi înțelese în sens larg drept orice metodă sau mijloc pe care îl poate folosi un operator în cadrul prelucrării. Prin *adecvate* se înțelege faptul că măsurile și garanțiile necesare trebuie să fie potrivite pentru realizarea scopului urmărit, adică trebuie să pună în aplicare *în mod eficace* principiile de protecție a datelor[3]. Cerința caracterului adecvat este, prin urmare, strâns legată de cerința eficacității.

9. O garanție și o măsură tehnică sau organizatorică poate consta în orice, de la utilizarea de soluții tehnice avansate până la pregătirea de bază a personalului. În funcție de context și de riscurile asociate prelucrării în cauză, pot reprezenta exemple potrivite pseudonimizarea datelor cu caracter

[3] „Eficacitatea” este abordată mai jos, în subcapitolul 2.1.2.

personal[4], stocarea datelor cu caracter personal disponibile într-un format structurat, utilizat în mod curent și care poate fi citit automat, posibilitatea ca persoanele vizate să intervină în procesul de prelucrare, furnizarea de informații privind stocarea datelor cu caracter personal, deținerea unor sisteme de depistare a programelor malware, instruirea angajaților cu privire la „igiena cibernetică" de bază, instituirea unor sisteme de management al confidențialității și al securității informațiilor, obligând contractual persoanele împuternicite de operator să pună în aplicare practici specifice de reducere la minimum a datelor etc.

10. Standardele, bunele practici și codurile de conduită recunoscute de asociații și de alte organisme care reprezintă categoriile de operatori de date pot ajuta la stabilirea măsurilor adecvate. Operatorul trebuie să verifice însă adecvarea măsurilor pentru prelucrarea specifică în cauză.

### 2.1.2 Destinată să pună în aplicare în mod eficace principiile de protecție a datelor și să protejeze drepturile și libertățile persoanelor vizate

11. *Principiile de protecție a datelor* sunt prezentate la articolul 5 (denumite în continuare „principiile"), iar *drepturile și libertățile persoanelor vizate* sunt drepturile fundamentale și libertățile persoanelor fizice, în special dreptul acestora la protecția datelor cu caracter personal, a căror protecție este precizată la articolul 1 alineatul (2) ca obiectiv al RGPD (denumite în continuare „drepturile")[5]. Formularea precisă a acestora se găsește în Carta drepturilor fundamentale a UE. Este esențial ca operatorul să înțeleagă ce semnifică *principiile* și *drepturile* ca bază pentru protecția oferită prin RGPD, în special prin obligația de asigurare a DPbDD.

12. La punerea în aplicare a măsurilor tehnice și organizatorice adecvate, măsurile și garanțiile trebuie *concepute* astfel încât să pună în aplicare în mod eficace fiecare dintre principiile sus-menționate și să protejeze drepturile în consecință.

**Abordarea eficacității**

13. Eficacitatea se află în centrul conceptului de protecție a datelor începând cu momentul conceperii. Cerința de punere în aplicare a principiilor într-un mod eficace presupune ca operatorii să pună în aplicare măsurile și garanțiile necesare pentru a proteja principiile respective, în vederea asigurării drepturilor persoanelor vizate. Fiecare măsură pusă în aplicare ar trebui să producă rezultatele urmărite pentru prelucrarea prevăzută de operator. Această observație are două consecințe.

14. În primul rând, înseamnă că articolul 25 nu impune punerea în aplicare a unor măsuri tehnice și organizatorice specifice, ci că măsurile și garanțiile alese trebuie să fie potrivite pentru punerea în aplicare a principiilor de protecție a datelor în cadrul prelucrării specifice în cauză. În acest proces, măsurile și garanțiile trebuie concepute să fie solide, iar operatorul trebuie să poată pune în aplicare măsuri suplimentare pentru a îmbunătăți protecția în cazul unei eventuale creșteri a riscurilor[6].

[4] Definită la articolul 4 alineatul (5) din RGPD.

[5] A se vedea considerentul 4 din RGPD.

[6] „Principiile fundamentale aplicabile operatorilor (respectiv legitimitatea, reducerea la minimum a datelor, limitarea scopului, transparența, integritatea datelor, exactitatea datelor) trebuie să rămână aceleași, indiferent de prelucrare și de riscurile pentru persoanele vizate. Cu toate acestea, atenția cuvenită în ceea ce privește natura și domeniul de aplicare a prelucrării respective au constituit dintotdeauna o parte integrantă a aplicării principiilor respective, astfel încât acestea să poată fi îmbunătățite în mod inerent." Grupul de lucru „Articolul 29". „Declarație privind rolul unei abordări bazate pe riscuri a cadrelor juridice privind protecția datelor". WP 218, 30 mai 2014, p 3. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

Eficacitatea măsurilor depinde așadar de contextul prelucrării respective și de evaluarea anumitor elemente care trebuie luate în considerate atunci când se determină mijloacele de prelucrare. Aceste elemente vor fi tratate mai jos, la subcapitolul 2.1.3.

15. În al doilea rând, operatorii trebuie să poată demonstra că principiile au continuat să fie respectate.

16. Garanțiile și măsurile puse în aplicare trebuie să obțină efectul scontat în materie de protecție a datelor, iar operatorul trebuie să dețină documentația măsurilor tehnice și organizatorice puse în aplicare[7]. Pentru aceasta, operatorul poate să stabilească indicatori-cheie de performanță (ICP) corespunzători pentru a demonstra eficacitatea. Un ICP este o valoare măsurabilă aleasă de operator, care demonstrează măsura în care realizează operatorul obiectivul stabilit privind protecția datelor. ICP pot fi *cantitativi*, precum procentajul de rezultate fals pozitive și fals negative, reducerea numărului de reclamații, reducerea timpului de răspuns când persoanele vizate își exercită drepturile, sau *calitativi*, precum evaluările performanței, utilizarea grilelor de notare sau evaluările de specialitate. În locul ICP, operatorii pot demonstra eficacitatea punerii în aplicare a principiilor argumentând modul în care au evaluat eficacitatea măsurilor și a garanțiilor selectate.

### 2.1.3 Elemente care trebuie luate în considerare

17. Articolul 25 alineatul (1) enumeră elementele pe care operatorul trebuie să le ia în considerare atunci când determină măsurile unei operațiuni de prelucrare specifice. În cele ce urmează, vă vom oferi orientări cu privire la modul de aplicare al acestor elemente în procesul de concepere, care include conceperea setărilor implicite. Toate aceste elemente contribuie la stabilirea adecvării sau a inadecvării unei măsuri pentru punerea în aplicare eficace a principiilor. Prin urmare, fiecare dintre aceste elemente reprezintă nu un obiectiv propriu-zis, ci un factor care trebuie avut în vedere pentru realizarea obiectivului.

#### *2.1.3.1 „stadiul actual al dezvoltării”/„stadiul actual al tehnologiei”*

18. Conceptul de „stadiu actual” al dezvoltării sau al tehnologiei este prezent în acquis-ul UE, de exemplu în ceea ce privește protecția mediului și siguranța produselor. În RGPD, „stadiul actual” al dezvoltării/tehnologiei[8] este menționat nu doar la articolul 32, în ceea ce privește măsurile de securitate[9][10], ci și la articolul 25, extinzând astfel acest criteriu de referință asupra tuturor măsurilor tehnice și organizatorice încorporate în cadrul prelucrării.

19. În contextul articolului 25, mențiunea „stadiul actual al tehnologiei” le impune operatorilor obligația ca, atunci când stabilesc măsurile tehnice și organizatorice adecvate, **să țină cont de progresul actual al tehnologiei** care este disponibilă pe piață. Aceasta cerință prevede ca operatorii să cunoască și să se mențină la curent cu progresele tehnologice, cu modul în care tehnologia poate prezenta riscuri sau oportunități în ceea ce privește protecția datelor pentru operațiunea de prelucrare, precum și cu

[7] A se vedea considerentele 74 și 78.

[8] A se vedea decizia din 1978 a Curții Constituționale Federale a Germaniei în cauza „Kalkar”: https://germanlawarchive.iuscomp.org/?p=67. Aceasta poate să ofere baza pentru o metodologie aplicabilă definirii obiective a conceptului. Pe acest temei, „stadiul actual al tehnologiei” ar fi identificat între nivelul tehnologic al „cunoștințelor și cercetării existente” și varianta mai recunoscută a „normelor tehnologice general acceptate”. Prin urmare, „stadiul actual al tehnologiei” poate fi identificat ca nivelul tehnologic al unui serviciu sau al unei tehnologii sau al unui produs care există pe piață și care este cel mai eficace în atingerea obiectivelor identificate.

[9] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security

[10] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

privire la modul de punere în aplicare și actualizare a măsurilor și a garanțiilor care *asigură punerea în aplicare eficace* a principiilor și a drepturilor persoanelor vizate având în vedere peisajul tehnologic în continuă evoluție.

20. „Stadiul actual al tehnologiei" este un concept dinamic, care nu poate fi definit în mod static într-un anumit moment, ci ar trebui evaluat *continuu* în contextul progresului tehnologic. Având în vedere progresele tehnologice, un operator ar putea constata că o măsură care oferea un nivel adecvat de protecție la un moment dat nu mai este suficientă la momentul actual. Prin urmare, neglijarea menținerii la curent în ceea ce privește schimbările tehnologice ar putea să aibă drept rezultat nerespectarea prevederilor articolului 25.

21. Criteriul legat de „stadiul actual al tehnologiei" nu se aplică doar măsurilor tehnologice, ci și celor organizatorice. Lipsa măsurilor organizatorice adecvate poate să scadă sau chiar să submineze complet eficacitatea tehnologiei alese. Adoptarea de politici interne, instruirea de actualitate în domeniul tehnologiei, al securității și al protecției datelor sau instituirea de politici de management și guvernanță a securității informatice pot reprezenta exemple de măsuri organizatorice.

22. Cadrele, standardele, certificatele, codurile de conduită etc. existente și recunoscute în diferite domenii pot avea un rol în indicarea „stadiului actual al tehnologiei" din cadrul domeniului de utilizare respectiv. În cazul în care există astfel de standarde care oferă un nivel înalt de protecție a persoanei vizate în conformitate cu cerințele juridice – sau chiar depășind aceste cerințe –, operatorii ar trebui să le ia în considerare la conceperea și punerea în aplicare a măsurilor de protecție a datelor.

#### *2.1.3.2 „costurile implementării"*

23. Operatorul poate să țină seama de costurile implementării la alegerea și aplicarea măsurilor tehnice și organizatorice adecvate și a garanțiilor necesare pentru punerea în aplicare eficace a principiilor menite să protejeze drepturile persoanelor vizate. Aceste costuri se referă la resurse în general, inclusiv la resursele de timp și la cele umane.

24. Elementul de cost nu impune operatorului să cheltuie o sumă disproporționată de resurse atunci când există măsuri alternative, mai puțin costisitoare dar eficace. Costurile implementării reprezintă un factor care trebuie avut în vedere la realizarea protecției datelor începând cu momentul conceperii, nu un motiv pentru care să nu realizeze protecția.

25. Prin urmare, măsurile alese trebuie să asigure faptul că activitatea de prelucrare prevăzută de operator prelucrează datele cu caracter personal fără a încălca principiile, indiferent de cost. Operatorii ar trebui să fie în măsură să gestioneze costurile totale astfel încât să poată pune în aplicare în mod eficace toate principiile și, astfel, să protejeze drepturile persoanelor.

#### *2.1.3.3 „natura, domeniul de aplicare, contextul și scopurile prelucrării"*

26. La stabilirea măsurilor necesare, operatorii trebuie să aibă în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării.

27. Acești factori trebuie interpretați în mod consecvent cu rolul lor din alte prevederi ale RGPD, cum ar fi articolele 24, 32 și 35, cu scopul de a configura procesul de prelucrare în jurul principiilor de protecție a datelor.

28. Pe scurt, conceptul de **natură** poate fi înțeles drept caracteristicile inerente[11] ale prelucrării. **Domeniul de aplicare** se referă la dimensiunea și la gama activităților de prelucrare. **Contextul** se referă la circumstanțele prelucrării, care pot influența așteptările persoanei vizate, în timp ce **scopurile** se referă la obiectivele prelucrării.

#### *2.1.3.4 „riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea"*

29. RGPD adoptă o abordare coerentă bazată pe riscuri în multe dintre dispozițiile sale, în articolele 24, 25, 32 și 35, cu scopul de a identifica măsuri tehnice și organizatorice adecvate pentru a proteja persoanele fizice și datele cu caracter personal ale acestora, respectând totodată cerințele RGPD. Activele care trebuie protejate sunt întotdeauna aceleași (persoanele fizice, prin protecția datelor cu caracter personal ale acestora) împotriva acelorași riscuri (riscurile la adresa drepturilor persoanelor), ținând cont de aceleași condiții (natura, domeniul de aplicare, contextul și scopurile prelucrării).

30. La efectuarea unei analize a riscurilor în vederea respectării articolului 25, operatorul trebuie să identifice riscurile pe care le presupune o încălcare a principiilor pentru drepturile persoanelor vizate și să stabilească probabilitatea și severitatea riscurilor identificate, pentru a pune în aplicare măsuri care să le reducă în mod eficace. Atunci când se efectuează evaluări ale riscurilor, o evaluare sistematică și aprofundată a prelucrării este crucială. De exemplu, un operator evaluează riscurile specifice asociate lipsei de consimțământ liber exprimat, ceea ce constituie o încălcare a principiului legalității, în cursul prelucrării datelor cu caracter personal ale copiilor și ale tinerilor sub 18 ani în calitate de categorie vulnerabilă, în cazul în care nu există alt temei juridic, și pune în aplicare măsuri adecvate pentru abordarea și reducerea eficace a riscurilor identificate asociate cu această categorie de persoane vizate.

31. „Orientările CEPD privind evaluarea impactului asupra protecției datelor (EIPD)"[12], care se concentrează asupra stabilirii probabilității ca o operațiune de prelucrare să genereze sau nu un risc ridicat pentru persoana vizată, oferă de asemenea orientări privind modul de evaluare a riscurilor pentru protecția datelor și cu privire la modul în care să se efectueze o evaluare a riscurilor pentru protecția datelor. Aceste orientări pot fi utile și în timpul evaluării riscurilor impuse de toate articolele menționate mai sus, inclusiv de articolul 25.

32. Abordarea bazată pe riscuri nu exclude utilizarea nivelurilor de referință, a bunelor practici și a standardelor. Acestea se pot dovedi a fi un set de instrumente util, cu ajutorul căruia operatorii pot aborda riscuri similare în situații similare (natura, domeniul de aplicare, contextul și scopurile prelucrării). Rămâne însă obligația de la articolul 25 [precum și de la articolul 24, articolul 32 și articolul 35 alineatul (7) litera (c)], de a ține cont de *„riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea"*. Prin urmare, operatorii, deși beneficiază de ajutorul unor astfel de instrumente, trebuie să efectueze întotdeauna o evaluare a riscurilor în ceea ce privește protecția datelor pentru activitatea de

[11] Menționăm ca exemple categoriile speciale de date cu caracter personal, procesele decizionale automate, relațiile de putere dezechilibrate, prelucrarea imprevizibilă, dificultățile întâmpinate de persoană vizată în exercitarea drepturilor etc.

[12] A se vedea Orientările Grupului de lucru „Articolul 29" 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". WP 248 rev. 01, 4 octombrie 2017. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 – aprobate de CEPD.

prelucrare în cauză și să verifice eficacitatea măsurilor și a garanțiilor adecvate propuse. În acest caz, este posibil să fie nevoie de încă o EIPD sau de o actualizare a EIPD existente.

### 2.1.4 Factorul timp

#### *2.1.4.1 În momentul stabilirii mijloacelor de prelucrare*

33. Protecția datelor începând cu momentul conceperii trebuie să fie realizată „*în momentul stabilirii mijloacelor de prelucrare*”.

34. „*Mijloacele de prelucrare*” variază de la elemente de proiectare generale până la cele detaliate ale prelucrării, incluzând arhitectura, procedurile, protocoalele, configurația și aspectul.

35. „*Momentul stabilirii mijloacelor de prelucrare*” se referă la intervalul de timp în care operatorul decide modul în care se va realiza prelucrarea și maniera în care va avea loc aceasta, precum și mecanismele care vor fi utilizate pentru efectuarea prelucrării respective. În cadrul acestui proces decizional, operatorul trebuie să evalueze măsurile și garanțiile adecvate în vederea punerii în aplicare în mod eficace a principiilor și a drepturilor persoanelor vizate în cadrul prelucrării, precum și să țină cont de elemente precum stadiul actual al tehnologiei, costurile implementării, natura, domeniul de aplicare, contextul și scopurile, precum și de riscuri. Tot aici se încadrează și momentul de achiziționare și implementare a programelor software, a hardware-ului și a serviciilor de prelucrare a datelor.

36. Luarea în considerare a DPbDD dintr-o etapă incipientă este crucială pentru punerea în aplicare cu succes a principiilor și pentru protejarea drepturilor persoanelor vizate. Mai mult, din punctul de vedere al raportului cost-beneficii, este și în interesul operatorilor să țină cont de DPbDD cât mai curând, întrucât poate să fie dificil și costisitor să se aducă schimbări ulterioare unor planuri deja făcute și unor operațiuni de prelucrare deja concepute.

#### *2.1.4.2 În momentul prelucrării în sine (menținerea și revizuirea cerințelor de protecție a datelor)*

37. Odată ce a fost inițiată prelucrarea, operatorul are în permanență obligația de a menține DPbDD, adică de a pune în aplicare constant și în mod eficace principiile pentru a proteja drepturile, de a fi la curent cu stadiul actual al tehnologiei, de a reevalua nivelul de risc etc. Natura, domeniul de aplicare și contextul operațiunilor de prelucrare, precum și riscul, pot suferi modificări în timpul prelucrării, ceea ce înseamnă că operatorul trebuie să-și reevalueze operațiunile de prelucrare prin revizuiri și evaluări periodice ale eficacității măsurilor și garanțiilor alese.

38. Obligația de menținere, revizuire și actualizare, după caz, a operațiunii de prelucrare se aplică și sistemelor preexistente. Aceasta înseamnă că sistemele existente, proiectate înainte de intrarea în vigoare a RGPD, trebuie să fie revizuite și întreținute astfel încât să asigure punerea în aplicare a unor măsuri și garanții care să pună în aplicare în mod eficace principiile și drepturile persoanelor vizate, astfel cum se subliniază în prezentele orientări.

39. Această obligație se extinde și asupra oricărei activități de prelucrare efectuate de persoanele împuternicite de operator. Operațiunile persoanelor împuternicite de operator trebuie să fie revizuite și evaluate în mod regulat de operatori, pentru a se asigura că fac posibilă respectarea continuă a principiilor și că îi permit operatorului de date să își îndeplinească obligațiile în acest sens.

## 2.2 Articolul 25 alineatul (2): Protecția datelor în mod implicit

### 2.2.1 În mod implicit, se prelucrează numai datele cu caracter personal care sunt necesare fiecărui scop specific al prelucrării

40. Un mod „implicit", așa cum este definit în mod obișnuit în informatică, se referă la valoarea preexistentă sau preselectată a unui parametru configurabil care este alocată unei aplicații software, unui program informatic sau unui dispozitiv. Acești parametri sunt denumiți și „setări prestabilite" sau „setări din fabrică", în special în cazul dispozitivelor electronice.

41. Prin urmare, termenul „în mod implicit" în cazul prelucrării datelor cu caracter personal se referă la alegerea valorilor de configurare sau a opțiunilor de prelucrare fixe sau prescrise într-un sistem de prelucrare, cum ar fi o aplicație software, un serviciu ori un dispozitiv, sau într-o procedură manuală de prelucrare și care afectează volumul de date cu caracter personal colectate, măsura în care sunt prelucrate, perioada de stocare și accesibilitatea acestora.

42. Operatorul trebuie să aleagă și să răspundă de punerea în aplicare a setărilor și a opțiunilor de prelucrare implicite astfel încât să se efectueze în mod implicit numai prelucrarea care este strict necesară pentru a atinge scopul stabilit și legal. Aici, operatorii ar trebui să se bazeze pe evaluarea proprie cu privire la necesitatea prelucrării în ceea ce privește temeiul juridic al articolului 6 alineatul (1). Aceasta înseamnă că, în mod implicit, operatorul trebuie să nu colecteze mai multe date decât este necesar, să nu prelucreze datele colectate mai mult decât este necesar scopului și să nu stocheze datele mai mult timp decât este necesar. Cerința de bază este ca protecția datelor să fie încorporată în mod implicit în prelucrare.

43. Operatorul are obligația de a stabili în prealabil în ce scopuri determinate, explicite și legitime sunt culese și prelucrate datele cu caracter personal[13]. Măsurile trebuie să fie în mod implicit adecvate, pentru a asigura prelucrarea doar a datelor cu caracter personal care sunt necesare în fiecare scop specific al prelucrării. „Orientările pentru evaluarea necesității și proporționalității măsurilor care limitează dreptul la protecția datelor cu caracter personal" ale AEPD pot fi utile și pentru a decide asupra datelor a căror prelucrare este necesară pentru a îndeplini un anumit scop[14] [15] [16].

44. În cazul în care utilizează un software produs de terți sau un software gata de utilizare, operatorul trebuie să efectueze o evaluare a riscului produsului și să se asigure că funcțiile care nu au un temei juridic sau care nu sunt compatibile cu scopurile propuse ale prelucrării sunt oprite.

45. Aceleași considerații se aplică măsurilor organizatorice care sprijină operațiunile de prelucrare. Acestea trebuie să fie concepute pentru a prelucra, la început, doar volumul minim de date cu caracter personal necesare pentru operațiunile respective. Acest lucru trebuie să fie luat în considerare în special când se alocă accesul la date unor membri ai personalului cu diferite roluri și cu nevoi de acces diferite.

[13] Articolul 5 alineatul (1) literele (b), (c), (d) și (e) din RGPD.

[14] AEPD. „Orientări privind evaluarea necesității și proporționalității măsurilor care limitează dreptul la protecția datelor". 25 februarie 2019. edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf

[15] A se vedea și AEPD. „Evaluarea necesității măsurilor care limitează dreptul fundamental la protecția datelor cu caracter personal: Set de instrumente" https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en

[16] Pentru mai multe informații privind necesitatea, a se vedea Grupul de lucru „Articolul 29". „Avizul 06/2014 privind noțiunea de interese legitime ale operatorului de date prevăzută la articolul 7 din Directiva 95/46/CE". WP 217, 9 aprilie 2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_ro.pdf

46. Prin urmare, „măsurile tehnice și organizatorice” adecvate, în contextul protecției implicite datelor în mod implicit, se interpretează în modul discutat mai sus în subcapitolul 2.1.1, dar se aplică în mod special la punerea în aplicare a principiului reducerii la minimum a datelor.

47. Obligația menționată anterior, de a prelucra numai datele cu caracter personal care sunt necesare pentru fiecare scop specific, se aplică următoarelor elemente.

### 2.2.2 Dimensiuni ale obligației de reducere la minimum a datelor

48. Articolul 25 alineatul (2) enumeră dimensiunile obligației de reducere la minimum a datelor pentru prelucrarea implicită, menționând că obligația se aplică volumului de date cu caracter personal colectate, măsurii în care acestea sunt prelucrate, perioadei în care sunt stocate și accesibilității acestora.

#### *2.2.2.1 „volumul de date colectate”*

49. Operatorii trebuie să ia în considerare atât volumul de date cu caracter personal, cât și tipurile, categoriile și nivelul de detaliu al datelor cu caracter personal necesare în scopul prelucrării. Alegerile în materie de proiectare trebuie să țină cont de riscurile sporite pentru principiul integrității și al confidențialității, de reducerea la minimum a datelor și de limitările legate de stocare atunci când se colectează volume mari de date cu caracter personal detaliate, iar toate acestea trebuie comparate cu reducerea riscurilor prin colectarea unor volume mai mici de informații și/sau a unor informații mai puțin detaliate despre persoanele vizate. Indiferent de situație, configurația implicită nu trebuie să includă colectarea de date cu caracter personal care nu sunt necesare pentru scopul specific al prelucrării. Cu alte cuvinte, dacă anumite categorii de date cu caracter personal nu sunt necesare sau dacă nu sunt necesare date detaliate pentru că este suficientă existența unor date mai puțin rafinate, atunci restul de date cu caracter personal nu se mai colectează.

50. Aceleași cerințe implicite se aplică serviciilor, indiferent de platforma sau dispozitivul în uz, putând fi colectate numai datele cu caracter personal necesare scopului propus.

#### *2.2.2.2 „gradul de prelucrare al acestora”*

51. Operațiunile de prelucrare[17] efectuate cu date cu caracter personal se limitează la ceea ce este necesar. Multe operațiuni de prelucrare pot contribui la îndeplinirea scopului prelucrării. Cu toate acestea, faptul că sunt necesare anumite date cu caracter personal pentru a îndeplini un scop nu înseamnă că datele respective pot fi supuse tuturor tipurilor de operațiuni de prelucrare, nici că pot fi prelucrate cu orice frecvență. De asemenea, operatorii trebuie să fie atenți să nu extindă limitele „scopurilor compatibile” de la articolul 6 alineatul (4) și să ia în considerare ceea ce se va situa în limitele așteptărilor rezonabile ale persoanelor vizate.

#### *2.2.2.3 „perioada lor de stocare”*

52. Datele cu caracter personal colectate nu trebuie stocate dacă nu sunt necesare scopului prelucrării și dacă nu există un alt scop și temei juridic compatibile, conform articolului 6 alineatul (4). Orice

[17] Conform articolului 4 alineatul (2) din RGPD, acestea includ colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.

păstrare a datelor trebuie să poată fi justificată de operator, în mod obiectiv, ca fiind necesară, în conformitate cu principiul responsabilității.

53. Operatorul trebuie să limiteze perioada de păstrare la ceea ce este necesar scopului. Dacă datele cu caracter personal nu mai sunt necesare scopului prelucrării, atunci vor fi șterse sau anonimizate în mod implicit. Prin urmare, perioada de păstrare va depinde de scopul prelucrării respective. Această obligație se leagă direct de principiul limitării legate de stocare de la articolul 5 alineatul (1) litera (e) și trebuie pusă în aplicare în mod implicit, în sensul că operatorul trebuie să aibă încorporate în prelucrare proceduri sistematice de ștergere sau anonimizare a datelor.

54. Anonimizarea[18] datelor cu caracter personal este o alternativă la ștergere, cu condiția ca toate elementele contextuale să fie luate în considerare și ca probabilitatea și gravitatea riscului, inclusiv a riscului de reidentificare, să fie evaluate în mod regulat[19].

#### *2.2.2.4 „accesibilitatea lor"*

55. Operatorul trebuie să limiteze persoanele care pot să aibă acces la datele cu caracter personal și tipurile de acces la aceste date în baza unei evaluări a necesității și, de asemenea, să se asigure că datele cu caracter personal sunt în mod real accesibile celor care au nevoie de ele când este necesar, de exemplu în situații critice. Măsurile de control al accesului trebuie să fie respectate pentru întregul flux de date din timpul prelucrării.

56. Articolul 25 alineatul (2) menționează în continuare că datele cu caracter personal nu trebuie să poată fi accesate, fără intervenția persoanei, de un număr nelimitat de persoane. Operatorul trebuie să limiteze în mod implicit accesibilitatea și să îi acorde persoanei vizate posibilitatea de a interveni înainte de a publica sau de a pune la dispoziție într-un alt mod date cu caracter personal despre persoana vizată unui număr nelimitat de persoane.

57. Punerea la dispoziție a datelor cu caracter personal unui număr nelimitat de persoane poate duce la o diseminare și mai mare a datelor decât s-a intenționat inițial, aspect relevant în special în contextul internetului și al motoarelor de căutare. Aceasta înseamnă că operatorii trebuie, în mod implicit, să ofere persoanelor vizate ocazia de a interveni înainte ca datele cu caracter personal să fie puse la dispoziție pe internetul deschis, aspect deosebit de important în cazul copiilor și al categoriilor vulnerabile.

58. În funcție de temeiurile juridice ale prelucrării, ocazia de a interveni ar putea varia în funcție de contextul prelucrării. De exemplu, poate să se solicite consimțământul pentru a face publice datele cu caracter personal sau pot să existe setări de confidențialitate astfel încât accesul public să poate fi controlat chiar de persoanele vizate.

[18] Grupul de lucru „Articolul 29". „Avizul 05/2014 privind tehnicile de anonimizare". WP 216, 10 aprilie 2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_ro.pdf

[19] A se vedea articolul 4 alineatul (1) din RGPD, considerentul 26 din RGPD, „Avizul 05/2014 privind tehnicile de anonimizare" al Grupului de lucru „Articolul 29". Consultați, de asemenea, subsecțiunea privind „limitările legate de stocare" din secțiunea 3 a prezentului document, care face referire la necesitatea ca operatorul să asigure eficacitatea tehnicii (tehnicilor) de anonimizare pusă (puse) în aplicare.

59. Chiar și în cazul în care datele cu caracter personal sunt puse la dispoziția publicului cu permisiunea și înțelegerea unei persoane vizate, aceasta nu înseamnă că orice alt operator care are acces la datele cu caracter personal le poate prelucra liber în regim propriu, în scopuri proprii – acesta trebuie să aibă propriul temei juridic[20].

# 3 PUNEREA ÎN APLICARE A PRINCIPIILOR DE PROTECȚIE A DATELOR ÎN PRELUCRAREA DATELOR CU CARACTER PERSONAL, FOLOSIND PROTECȚIA DATELOR DIN FAZA DE PROIECTARE ȘI PROTECȚIA IMPLICITĂ A DATELOR

60. În toate etapele de proiectare a activităților de prelucrare, inclusiv în achiziții, licitații, procese de externalizare, dezvoltare, asistență, întreținere, testare, stocare, ștergere etc., operatorul trebuie să ia în considerare și să analizeze diferitele elemente ale DPbDD, pentru care se vor oferi exemple în acest capitol, în contextul punerii în aplicare a principiilor[21] [22] [23].

61. Operatorii trebuie să pună în aplicare principiile pentru a realiza DPbDD. Aceste principii sunt: transparența, legalitatea, echitatea, limitarea scopului, reducerea la minimum a datelor, exactitatea, limitările legate de stocare, integritatea și confidențialitatea, responsabilitatea. Principiile respective sunt evidențiate la articolul 5 și în considerentul 39 din RGPD. Pentru a înțelege pe deplin modul de punere în aplicare a DPbDD, se pune accentul pe importanța înțelegerii semnificației fiecărui principiu.

62. La prezentarea exemplelor privind modul de operaționalizare a DPbDD, am întocmit liste ale **principalelor elemente legate de DPbDD** pentru fiecare principiu. Exemplele, deși subliniază principiul specific al protecției datelor în discuție, se pot suprapune și cu alte principii aflate în strânsă legătură cu acesta. CEPD subliniază că elementele principale și exemplele prezentate mai jos nu sunt nici exhaustive, nici obligatorii, ci au rolul unor elemente de orientare pentru fiecare principiu în parte. Operatorii trebuie să evalueze modul în care pot garanta respectarea principiilor în contextul operațiunii concrete de prelucrare respective.

63. Secțiunea de față se axează pe punerea în aplicare a principiilor, însă operatorul trebuie să pună în aplicare de asemenea metode *adecvate* și *eficace* care să protejeze drepturile persoanelor vizate, în conformitate cu capitolul III din RGPD, în cazul în care acest lucru nu este deja impus de principiile propriu-zise.

64. Responsabilitatea este un principiu general: presupune ca operatorul să răspundă de alegerea măsurilor tehnice și organizatorice necesare.

[20] A se vedea cauza Satakunnan Markkinapörssi Oy și Satamedia Oy/Finlanda, nr. 931/13.
[21] Mai multe exemple se găsesc în documentul Autorității norvegiene pentru protecția datelor, „Dezvoltarea de software cu asigurarea protecției datelor începând cu momentul conceperii și în mod implicit”. 28 noiembrie 2017. www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729
[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers
[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

## 3.1 Transparență[24]

65. Operatorul trebuie să informeze clar și deschis persoana vizată cu privire la modul în care va colecta, utiliza și distribui datele cu caracter personal. Transparența se referă la posibilitatea pe care o au persoanele vizate de a înțelege și, dacă este necesar, de a-și exercita drepturile din articolele 15-22. Principiul este încorporat în articolele 12, 13, 14 și 34. Măsurile și garanțiile puse în aplicare pentru a sprijini principiul transparenței trebuie să sprijine și punerea în aplicare a acestor articole.

66. Exemple de elemente principale legate de concepere și de protecția implicită menite să asigure transparența:

- Claritatea - Informațiile sunt formulate într-un limbaj clar și simplu, concis și inteligibil.
- Semantica - Comunicarea trebuie să aibă un sens clar pentru publicul în cauză.
- Accesibilitatea - Informațiile sunt ușor accesibile pentru persoana vizată.
- Contextualitatea - Informațiile se furnizează în momentul relevant și în forma corespunzătoare.
- Relevanța - Informațiile trebuie să fie relevante și aplicabile respectivei persoane vizate.
- Proiectarea universală - Informațiile sunt accesibile tuturor persoanelor vizate, inclusiv prin utilizarea limbajelor citibile automat pentru a facilita și automatiza claritatea.
- Nivelul de înțelegere - Persoanelor vizate trebuie să le fie suficient de clar la ce se pot aștepta în ceea ce privește prelucrarea datelor lor cu caracter personal, în special atunci când persoanele vizate sunt copii sau alte grupuri vulnerabile.
- Canale multiple - Informațiile trebuie să fie furnizate pe canale și prin mijloace diferite, nu numai sub formă textuală, pentru a spori probabilitatea ca informațiile să ajungă efectiv la persoana vizată.
- Mai multe niveluri – Informațiile trebuie structurate într-un mod care să soluționeze tensiunea dintre caracterul complet și înțelegere, ținând cont totodată de așteptările rezonabile ale persoanelor vizate.

Exemplu[25]

Un operator concepe pentru site-ul său o politică de confidențialitate, cu scopul de a respecta cerințele privind transparența. Politica de confidențialitate nu trebuie să conțină un volum mare de informații care sunt dificil de parcurs și de înțeles de către o persoană vizată obișnuită. Ea trebuie să fie scrisă într-un limbaj clar și concis și să ajute utilizatorul site-ului să înțeleagă modul în care îi sunt prelucrate datele cu caracter personal. Prin urmare, operatorul oferă informații într-un mod structurat, în care sunt evidențiate cele mai importante puncte. Informațiile mai detaliate pot fi accesate ușor. Se oferă meniuri derulante și linkuri către alte pagini pentru a explica mai detaliat diversele articole și concepte utilizate în cadrul politicii. De asemenea, operatorul se asigură că informațiile sunt furnizate pe mai multe canale, oferind videoclipuri pentru a explica aspectele cele mai importante ale informării scrise. Sinergia dintre diversele pagini este vitală pentru asigurarea faptului că abordarea pe mai multe niveluri nu sporește confuzia, ci o reduce.

[24] O detaliere a modului în care trebuie înțeles conceptul transparenței se găsește în documentul Grupului de lucru „Articolul 29", „Orientări privind transparența în temeiul Regulamentului 2016/679". WP 260 rev. 01, 11 aprilie 2018. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 - aprobate de CEPD

[25] Autoritatea franceză pentru protecția datelor a publicat câteva exemple, ilustrând bunele practici în ceea ce privește informarea utilizatorilor, precum și alte principii de transparență: https://design.cnil.fr/en/.

Politica de confidențialitate nu trebuie să fie greu de accesat de către persoanele vizate. De aceea, politica de confidențialitate este pusă la dispoziție și vizibilă pe toate paginile site-ului în discuție, astfel încât persoana vizată să fie în permanență la un clic distanță de accesarea informațiilor. Informațiile furnizate sunt concepute, de asemenea, în conformitate cu bunele practici și cu standardele de proiectare universală pentru a le face accesibile tuturor.

În plus, informațiile necesare trebuie să fie furnizate în contextul potrivit, la momentul adecvat. Având în vedere că operatorul efectuează mai multe operațiuni de prelucrare utilizând datele colectate pe site, doar o politică de confidențialitate generală pe site-ul respectiv nu este suficientă pentru ca operatorul să îndeplinească cerințele privind transparența. Prin urmare, operatorul concepe un flux de informații, prezentându-i persoanei vizate informațiile relevante în contextele adecvate, folosind, de exemplu, extrase informative sau mesaje pop-up. De exemplu, atunci când solicită persoanei vizate să introducă date cu caracter personal, operatorul o informează cu privire la modul în care vor fi prelucrate și cu privire la motivul pentru care sunt necesare datele cu caracter personal pentru prelucrare.

## 3.2 Legalitate

67. Operatorul trebuie să identifice un temei juridic valid pentru prelucrarea datelor cu caracter personal. Măsurile și garanțiile trebuie să sprijine cerința de a asigura faptul că întregul ciclu de prelucrare se conformează temeiurilor juridice relevante ale prelucrării.

68. Exemple de elemente principale legate de concepere și de protecția implicită menite să asigure legalitatea:
    - Relevanța – Se aplică temeiul juridic corect activității de prelucrare.
    - Diferențierea[26] – Se diferențiază temeiul juridic utilizat pentru fiecare activitate de prelucrare.
    - Scopul specificat – Temeiul juridic adecvat trebuie să se lege în mod clar de scopul specific al prelucrării[27].
    - Caracterul necesar – Prelucrarea trebuie să fie necesară și necondiționată pentru ca scopul să fie legal.
    - Autonomia – Persoanei vizate trebuie să i se acorde cel mai înalt grad de autonomie posibil în ceea ce privește controlul asupra datelor cu caracter personal, în limitele temeiului juridic.
    - Obținerea consimțământului – consimțământul trebuie să fie liber exprimat, specific, în cunoștință de cauză și clar[28]. Trebuie acordată o atenție deosebită capacității copiilor și tinerilor de a-și da consimțământul în cunoștință de cauză.
    - Retragerea consimțământului – În cazul în care consimțământul reprezintă temeiul juridic, prelucrarea trebuie să faciliteze retragerea consimțământului. Retragerea consimțământului

[26] CEPD, „Orientările 2/2019 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (b) din RGPD în contextul furnizării de servicii online persoanelor vizate". Versiunea 2.0, 8 octombrie 2019. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_ro.pdf

[27] A se vedea secțiunea privind limitările legate de scop de mai jos.

[28] A se vedea Orientările 05/2020 privind consimțământul în baza Regulamentului 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

trebuie să fie la fel de simplă ca acordarea acestuia. În caz contrar, mecanismul privind consimțământul al operatorului nu respectă RGPD[29].

- Echilibrarea intereselor – În cazul în care interesele legitime reprezintă temeiul juridic, operatorul trebuie să realizeze o echilibrare ponderată a interesului, acordând o atenție deosebită dezechilibrului de putere, în special în cazul copiilor cu vârsta sub 18 ani și al altor categorii vulnerabile. Trebuie să existe măsuri și garanții care să reducă impactul negativ asupra persoanelor vizate.
- Prestabilirea - Temeiul legal se stabilește înainte să aibă loc prelucrarea.
- Încetarea - Dacă temeiul juridic încetează să fie aplicabil, prelucrarea poate să înceteze în consecință.
- Ajustarea - Dacă există o modificare validă a temeiului juridic al prelucrării, prelucrarea efectivă trebuie ajustată în conformitate cu noul temei juridic[30].
- Alocarea răspunderii - Ori de câte ori se are în vedere un control comun, părțile trebuie să își împartă într-un mod clar și transparent responsabilitățile față de persoana vizată și să conceapă măsurile de prelucrare în conformitate cu această alocare.

Exemplu

O bancă intenționează să ofere un serviciu menit să îmbunătățească eficiența în gestionarea cererilor de împrumut. Ideea care stă la baza acestui serviciu este aceea ca banca, solicitând permisiunea clientului, să poată obține date despre client direct de la autoritățile fiscale publice. Acest exemplu nu are în vedere prelucrarea datelor cu caracter personal din alte surse.

Pentru a continua demersurile inițiate prin cererea persoanei vizate de a încheia un contract de împrumut, este necesară obținerea unor date cu caracter personal referitoare la situația financiară a persoanei vizate[31]. Cu toate acestea, nu se consideră că este necesară obținerea datelor cu caracter personal direct de la administrația fiscală, deoarece clientul poate încheia un contract furnizând el însuși aceste informații obținute de la administrația fiscală. Deși interesul băncii în obținerea documentației direct de la autoritățile fiscale poate fi legitim, de exemplu pentru a eficientiza prelucrarea împrumutului, acordarea de acces direct băncilor la datele cu caracter personal ale solicitanților dă naștere unui risc legat de utilizarea sau potențiala utilizare abuzivă a drepturilor de acces.

La punerea în aplicare a principiului legalității, operatorul își dă seama că, în acest context, nu poate utiliza temeiul „necesar pentru contract” pentru acea parte a prelucrării care presupune colectarea de date cu caracter personal direct de la autoritățile fiscale. Faptul că această prelucrare specifică prezintă riscul ca persoana vizată să devină mai puțin implicată în prelucrarea datelor sale este, de asemenea, un factor relevant în evaluarea legalității prelucrării în sine. Banca concluzionează că această parte a prelucrării trebuie să se bazeze pe un alt temei juridic. În statul membru specific în care se află operatorul există legi naționale care permit băncii să obțină informații direct de la autoritățile fiscale publice, în cazul în care persoana vizată își dă consimțământul înainte.

[29] A se vedea Orientările 05/2020 privind consimțământul în baza Regulamentului 2016/679, p 24. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[30] În cazul în care temeiul juridic original este consimțământul, a se vedea Orientările 05/2020 privind consimțământul în baza Regulamentului 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[31] A se vedea articolul 6 alineatul (1) litera (b) din RGPD.

Prin urmare, banca prezintă informații cu privire la prelucrare pe platforma online pe care se depun cererile, în așa fel încât persoanele vizate să înțeleagă cu ușurință care activități de prelucrare sunt obligatorii și care sunt opționale. Opțiunile de prelucrare, în mod implicit, nu permit extragerea de date din alte surse decât chiar de la persoana vizată, iar opțiunea de extragere directă a informațiilor este prezentată într-un mod care nu împiedică persoana vizată să îl refuze. Consimțământul acordat pentru colectarea de date direct de la alți operatori este un drept de acces temporar la un set specific de informații.

Orice consimțământ acordat este prelucrat electronic într-un mod care poate fi documentat, iar persoanelor vizate li se oferă o modalitate simplă prin care pot controla aspectele cu privire la care și-au acordat consimțământul și prin care își pot retrage consimțământul.

Operatorul a evaluat în prealabil aceste cerințe privind DPbDD și include toate aceste criterii în caietul de sarcini pe care îl întocmește pentru licitația destinată achiziționării platformei. Operatorul știe că dacă nu include cerințele privind DPbDD în licitație, punerea în aplicare ulterioară a protecției datelor poate să intervină prea târziu sau poate să fie un proces foarte costisitor.

## 3.3 Echitate

69. Echitatea este un principiu general, care impune ca datele cu caracter personal să nu fie prelucrate într-un mod dăunător fără justificare, discriminator fără bază legală, neașteptat sau înșelător pentru persoana vizată. Măsurile și garanțiile prin care se pune în aplicare principiul echității sprijină totodată drepturile și libertățile persoanelor vizate, în special dreptul la informare (transparență), dreptul de a interveni (acces, ștergere, portabilitatea datelor, rectificare) și dreptul de a limita prelucrarea (dreptul de a nu face obiectul unor procese decizionale automatizate și nediscriminarea persoanelor vizate în aceste procese).

70. Exemple de elemente principale legate de concepere și de protecția implicită menite să asigure echitatea:
    - Autonomia – Persoanelor vizate trebuie să li se acorde cel mai înalt nivel posibil de autonomie pentru a stabili modul în care le sunt utilizate datele cu caracter personal, precum și domeniul de aplicare și condițiile utilizării sau prelucrării respective.
    - Interacțiunea - Persoanele vizate trebuie să aibă posibilitatea de a comunica și de a-și exercita drepturile în ceea ce privește datele cu caracter personal prelucrate de operator.
    - Așteptările - Prelucrarea trebuie să corespundă așteptărilor rezonabile ale persoanelor vizate.
    - Nediscriminarea - Operatorul nu discriminează pe nedrept persoanele vizate.
    - Neexploatarea - Operatorul nu exploatează necesitățile sau vulnerabilitățile persoanelor vizate.
    - Posibilitățile de alegere ale consumatorilor - Operatorul nu trebuie să creeze în mod neloial o „dependență” a utilizatorilor. Ori de câte ori un serviciu care prelucrează date cu caracter personal este unul exclusiv, se poate crea o „dependență” de serviciul respectiv, care poate să fie neloială în cazul în care afectează posibilitatea persoanelor vizate de a-și exercita dreptul la portabilitatea datelor în conformitate cu articolul 20.
    - Echilibrul puterii – Echilibrul puterii trebuie să fie un obiectiv esențial al relației dintre operator și persoana vizată. Dezechilibrele de putere trebuie evitate, iar atunci când nu este posibil, acestea trebuie recunoscute și contracarate prin contramăsuri adecvate.

- Fără transferuri ale riscurilor – Operatorii nu trebuie să transfere riscurile întreprinderii către persoanele vizate.
- Fără înșelătorii – Informațiile și opțiunile privind prelucrarea datelor trebuie oferite într-un mod obiectiv și neutru, evitându-se orice terminologie sau structură înșelătoare sau manipulatoare.
- Respectarea drepturilor – Operatorul trebuie să respecte drepturile fundamentale ale persoanelor vizate, să pună în aplicare măsuri și garanții adecvate și să nu afecteze aceste drepturi, cu excepția cazului în care este justificat în mod expres prin lege.
- Caracterul etic - Operatorul trebuie să ia în considerare impactul mai amplu pe care îl are prelucrarea asupra drepturilor și asupra demnității persoanelor fizice.
- Corectitudinea – Operatorul trebuie să pună la dispoziție informații despre modul în care prelucrează datele cu caracter personal, să acționeze conform celor declarate și să nu inducă în eroare persoanele vizate.
- Intervenția umană - Operatorul trebuie să încorporeze intervenție umană *calificată*, capabilă să descopere erorile sistematice pe care le pot crea mașinile, în conformitate cu dreptul de a nu face obiectul procesului decizional individual automatizat menționat la articolul 22[32].
- Algoritmii echitabili – Trebuie să se evalueze cu regularitate dacă algoritmii funcționează în conformitate cu scopurile, să se ajusteze algoritmii pentru reducerea erorilor sistematice descoperite și să se asigure echitatea prelucrării. Persoanele vizate trebuie să fie informate cu privire la funcționarea prelucrării datelor cu caracter personal în baza algoritmilor care analizează sau fac predicții despre acestea, de exemplu despre randamentul la locul de muncă, situația economică, starea de sănătate, preferințele personale, fiabilitatea sau comportamentul, locația sau deplasările persoanei[33].

Exemplul 1

Un operator folosește un motor de căutare care prelucrează în principal date cu caracter personal generate de utilizator. Operatorul are anumite beneficii de pe urma deținerii unor cantități mari de date cu caracter personal și a capacității de a folosi datele respective pentru reclame țintite. Prin urmare, operatorul dorește să influențeze persoanele vizate pentru ca acestea să permită colectarea și utilizarea mai amplă a datelor lor cu caracter personal. Consimțământul se obține prezentând persoanei vizate diversele opțiuni privind prelucrarea.

În momentul în care pune în aplicare principiul echității, ținând cont de natura, domeniul de aplicare, contextul și scopurile prelucrării, operatorul își dă seama că nu poate prezenta opțiunile într-un mod care să împingă persoana vizată înspre a-i permite operatorului să colecteze mai multe date cu caracter personal decât dacă opțiunile ar fi prezentate într-un mod egal și neutru. Aceasta înseamnă că nu poate prezenta opțiunile de prelucrare în așa fel încât persoanelor vizate să le fie dificil să refuze comunicarea datelor sau astfel încât persoanelor vizate să le fie dificil să-și ajusteze setările de confidențialitate pentru a limita prelucrarea. Acestea sunt exemple de tipare negative, care contravin spiritului articolului 25. Opțiunile implicite pentru prelucrare nu trebuie să fie invazive, iar opțiunea de prelucrare ulterioară trebuie să fie prezentată într-un mod care să nu preseze persoana vizată să

[32] A se vedea Orientările privind procesul decizional individual automatizat și crearea de profiluri în sensul Regulamentului (UE) 2016/679. https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826

[33] A se vedea considerentul 71 din RGPD.

își dea consimțământul. Prin urmare, operatorul prezintă opțiunile de a consimți sau de a refuza ca pe două alegeri cu vizibilitate egală, prezentând cu exactitate persoanei vizate ramificațiile fiecărei alegeri.

Exemplul 2

Un alt operator prelucrează date cu caracter personal pentru furnizarea unui serviciu de streaming, în cadrul căruia utilizatorii pot alege între un abonament simplu, de calitate standard, și un abonament premium, de o calitate mai bună. În cadrul abonamentului premium, abonații beneficiază de servicii prioritare de relații cu clienții.

În ceea ce privește principiul echității, serviciul prioritar de relații cu clienții acordat abonaților premium nu poate să discrimineze accesul abonaților obișnuiți la exercitarea drepturilor lor, conform articolului 12 din RGPD. Aceasta înseamnă că, deși abonații premium beneficiază de un serviciu prioritar, această prioritate nu trebuie să aibă drept rezultat o lipsă a măsurilor adecvate pentru a răspunde la solicitările abonaților standard fără întârzieri nejustificate și, indiferent de situație, în termen de o lună de la primirea solicitărilor.

Clienții prioritari pot să plătească pentru a obține un serviciu mai bun, însă toate persoanele vizate trebuie să aibă acces egal și nediscriminat pentru a se asigura de respectarea drepturilor și libertăților avute, astfel cum se prevede la articolul 12.

## 3.4 Limitări legate de scop[34]

71. Operatorul trebuie să colecteze date în scopuri determinate, explicite și legitime și să nu prelucreze datele ulterior într-un mod incompatibil cu scopurile în care au fost colectate[35]. Prin urmare, activitatea de prelucrare trebuie concepută în funcție de ceea ce este necesar pentru a îndeplini scopurile. Dacă trebuie să se realizeze o prelucrare ulterioară, operatorul trebuie să se asigure mai întâi că această prelucrare are scopuri compatibile cu cele inițiale și să conceapă această activitate de prelucrare în consecință. Caracterul compatibil sau incompatibil al unui nou scop trebuie să fie evaluat în conformitate cu criteriile de la articolul 6 alineatul (4).

72. Exemple de elemente principale legate de concepere și de protecția implicită menite să asigure limitarea scopului:
    - Prestabilirea - Scopurile legitime trebuie să fie stabilite înainte de proiectarea prelucrării.
    - Specificitatea – Scopurile trebuie să fie specificate și explicite în legătură cu motivul prelucrării datelor cu caracter personal.
    - Orientarea către scop - Scopul prelucrării trebuie să ghideze conceptul prelucrării și să stabilească limitele prelucrării.
    - Necesitatea - Scopul determină datele cu caracter personal care sunt necesare pentru prelucrare.

[34] Grupul de lucru „Articolul 29” a oferit orientări pentru înțelegerea principiului limitărilor legate de scop în temeiul Directivei 95/46/CE. Deși avizul nu este adoptat de CEPD, poate să fie totuși relevant, întrucât formularea principiului este aceeași în cadrul RGPD. Grupul de lucru „Articolul 29”, „Avizul 03/2013 privind limitările legate de scop”. WP 203, 2 aprilie 2013. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[35] Articolul 5 alineatul (1) litera (b) din RGPD.

- Compatibilitatea - Orice scop nou trebuie să fie compatibil cu scopul inițial pentru care s-au colectat datele și să determine schimbări relevante în modul de concepere a prelucrării.
- Limitarea prelucrării ulterioare - Operatorul trebuie să nu facă legături între seturile de date și să nu efectueze prelucrări suplimentare în scopuri noi incompatibile.
- Limitările reutilizării - Operatorul trebuie să utilizeze măsuri tehnice, inclusiv hashingul și criptarea, pentru a limita posibilitatea ca datele cu caracter personal să fie folosite în alte scopuri. De asemenea, operatorul trebuie să aibă instituite măsuri organizatorice, cum ar fi politici și obligații contractuale, care să limiteze reutilizarea datelor cu caracter personal.
- Revizuirea - Operatorul trebuie să analizeze în mod regulat dacă prelucrarea este necesară pentru scopurile în care au fost colectate datele și să testeze modul de concepere a prelucrării în raport cu limitările legate de scop.

Exemplu

Operatorul prelucrează date cu caracter personal despre clienții săi. Scopul prelucrării este acela de a executa un contract, respectiv de a putea livra bunuri la adresa corectă și de a obține plata. Datele cu caracter personal stocate sunt istoricul achizițiilor, numele, adresa, adresa de e-mail și numărul de telefon.

Operatorul se gândește să cumpere un produs de gestionare a relațiilor cu clienții (CRM), care colectează toate datele privind clienții legate de activitatea de vânzări, de marketing și de servicii pentru clienți într-un singur loc. Produsul oferă posibilitatea de a stoca toate apelurile telefonice, activitățile, documentele, e-mailurile și campaniile de marketing, pentru a obține o imagine completă despre client. Mai mult, CRM poate analiza automat puterea de cumpărare a clienților, folosind informații publice. Scopul analizei este acela de a direcționa mai bine activitățile de publicitate. Activitățile din urmă nu fac parte din scopul legal inițial al prelucrării.

Pentru a se conforma principiului limitărilor legate de scop, operatorul îi solicită furnizorului produsului să inventarieze diferitele activități de prelucrare care folosesc date cu caracter personal, suprapunându-le peste scopurile relevante pentru operator.

După primirea rezultatelor inventarierii, operatorul evaluează dacă noul scop legat de marketing și scopul legat de reclamele țintite sunt compatibile cu scopurile inițiale definite la momentul colectării datelor și dacă există suficient temei juridic pentru prelucrarea respectivă. Dacă evaluarea nu are un răspuns pozitiv, operatorul nu va utiliza funcționalitățile respective. Alternativ, operatorul poate alege să renunțe la evaluare și pur și simplu să nu utilizeze funcționalitățile descrise ale produsului.

## 3.5 Reducerea la minimum a datelor

73. Se prelucrează doar datele cu caracter personal care sunt adecvate, relevante și limitate la ceea ce este **necesar** în raport cu scopurile[36]. Prin urmare, operatorul trebuie să stabilească în prealabil ce caracteristici și parametri ai sistemelor de prelucrare și ce funcții de sprijin ale acestora sunt permisibile. Reducerea la minimum a datelor fundamentează și pune în practică principiul necesității. În cadrul prelucrării ulterioare, operatorul trebuie să analizeze periodic dacă datele cu caracter personal prelucrate sunt în continuare adecvate, relevante și necesare sau trebuie să fie șterse sau anonimizate.

[36] Articolul 5 alineatul (1) litera (c) din RGPD.

74. Operatorii trebuie să stabilească în primul rând dacă este cu adevărat nevoie să prelucreze date cu caracter personal în scopurile relevante respective. Operatorul trebuie să verifice dacă scopurile relevante pot fi realizate prin prelucrarea unui volum mai mic de date cu caracter personal sau a unor date cu caracter personal mai puțin detaliate sau agregate sau fără să fie nevoie să prelucreze date cu caracter personal[37]. Această verificare ar trebui să aibă loc înaintea oricărei activități de prelucrare, însă ar putea fi efectuată oricând în cursul prelucrării. Aceste aspecte sunt de asemenea conforme cu dispozițiile articolului 11.

75. Reducerea la minimum se poate referi și la gradul de identificare. Dacă scopul prelucrării nu necesită ca setul final de date să facă referire la o persoană fizică identificată sau identificabilă (un exemplu în acest sens sunt statisticile), însă prelucrarea inițială presupune acest lucru (de exemplu înainte de agregarea datelor), atunci operatorul șterge sau anonimizează datele cu caracter personal de îndată ce identificarea nu mai este necesară. Sau, în cazul în care identificarea în continuare este necesară pentru alte activități de prelucrare, datele cu caracter personal trebuie să fie pseudonimizate, pentru a atenua riscurile pentru drepturile persoanelor vizate.

76. Exemple de elemente principale legate de concepere și de protecția implicită menite să asigure reducerea la minimum a datelor:
    - Evitarea datelor – Evitarea pe deplin a prelucrării datelor cu caracter personal când acest lucru este posibil în scopul relevant.
    - Limitarea - Limitarea volumului de date colectate la ceea ce este necesar pentru scopul respectiv
    - Limitarea accesului - Configurarea prelucrării datelor astfel încât un număr minim de persoane să aibă nevoie de acces la datele cu caracter personal pentru a-și îndeplini sarcinile și limitarea accesului în consecință.
    - Relevanța - Datele cu caracter personal trebuie să fie relevante pentru prelucrarea în cauză, iar operatorul trebuie să poată demonstra această relevanță.
    - Necesitatea - Fiecare categorie de date cu caracter personal este necesară în scopurile determinate și trebuie prelucrată doar dacă nu este posibil să se îndeplinească scopul prin alte mijloace.
    - Agregarea - Utilizarea de date agregate atunci când este posibil.
    - Pseudonimizarea - Pseudonimizarea datelor cu caracter personal imediat ce nu mai este necesar să se dețină date cu caracter personal direct identificabile și stocarea separată a cheilor de identificare.
    - Anonimizarea și ștergerea - În cazul în care datele cu caracter personal nu sunt necesare sau nu mai sunt necesare în scopul respectiv, datele cu caracter personal trebuie să fie anonimizate sau șterse.
    - Fluxul de date - Fluxul de date trebuie să fie suficient de eficient încât să nu se creeze mai multe copii decât este necesar.
    - „Stadiul actual al tehnologiei” - Operatorul trebuie să aplice tehnologii actuale și adecvate pentru evitarea și reducerea la minimum a datelor.

Exemplul 1

[37] Considerentul 39 din RGPD menționează următoarele: „[...] Datele cu caracter personal ar trebui prelucrate doar dacă scopul prelucrării nu poate fi îndeplinit în mod rezonabil prin alte mijloace”.

O librărie dorește să își sporească veniturile comercializându-și cărțile online. Proprietarul librăriei dorește să stabilească un formular standardizat pentru procesul de plasare a comenzilor. Pentru a se asigura că clienții completează toate informațiile dorite, proprietarul librăriei setează toate câmpurile din formular drept câmpuri obligatorii (dacă nu se completează toate câmpurile, clientul nu poate plasa comanda). Proprietarul magazinului online folosește inițial un formular de contact standard, în care se solicită informații precum data nașterii clientului, numărul de telefon și adresa de domiciliu. Nu toate câmpurile din formular sunt însă necesare în scopul cumpărării și al livrării cărților. În acest caz specific, dacă persoana vizată plătește produsul pe loc, data nașterii și numărul de telefon al persoanei vizate nu sunt necesare pentru achiziționarea produsului. Câmpurile respective din formularul web nu pot fi așadar câmpuri obligatorii pentru plasarea comenzii, cu excepția cazului în care în care operatorul poate să demonstreze în mod clar că sunt necesare în alte scopuri, explicând motivul pentru care sunt necesare. În plus, există situații în care adresa nu este necesară. De exemplu, la comandarea unei cărți electronice, clientul poate să descarce produsul direct pe dispozitiv.

Prin urmare, proprietarul magazinului online decide să întocmească două formulare web: unul pentru comenzile de cărți tipărite, cu un câmp pentru adresa clientului, și un formular web pentru comenzile de cărți electronice, fără un câmp pentru adresa clientului.

Exemplul 2

O companie de transport în comun dorește să colecteze informații statistice în baza rutelor de călătorie. Acest lucru este util în scopul efectuării unor alegeri adecvate în ceea ce privește modificarea programelor de transport în comun și stabilirea unor rute corespunzătoare ale trenurilor. Pasagerii trebuie să își treacă biletul printr-un cititor de fiecare dată când intră într-un mijloc de transport sau ies din acesta. După efectuarea unei evaluări a riscurilor legate de drepturile și libertățile pasagerilor ca urmare a colectării de date privind rutele de călătorie, operatorul stabilește că este posibilă identificarea pasagerilor care locuiesc sau muncesc în zone puțin populate, datorită codului de identificare a biletelor folosite pe o singură rută. Prin urmare, întrucât nu este necesar în scopul optimizării programelor de transport în comun și al rutelor trenurilor, operatorul nu stochează codul de identificare a biletului. După ce se încheie călătoria, operatorul stochează doar rutele de călătorie individuale, ca să nu poată să identifice călătoriile legate de un singur bilet, dar păstrează doar informații despre rute de călătorie separate.

În cazurile în care poate totuși să existe un risc de identificare a unei persoane exclusiv în baza rutei sale de călătorie cu transportul public, operatorul pune în aplicare măsuri statistice pentru reducerea riscului, cum ar fi eliminarea începutului și a sfârșitului rutei.

Exemplul 3

O firmă de curierat își propune să evalueze eficacitatea activității sale din punctul de vedere al timpilor de livrare, al programării volumului de muncă și al consumului de combustibil. Pentru a îndeplini acest obiectiv, firma de curierat trebuie să prelucreze o serie de date cu caracter personal legate atât de angajați (șoferi), cât și de clienți (adrese, articole de livrat etc.). Această operațiune de prelucrare implică riscuri atât privind monitorizarea angajaților, care necesită garanții legale specifice, cât și privind urmărirea obiceiurilor clienților prin cunoștințele despre articolele livrate de-a lungul timpului. Aceste riscuri pot fi reduse în mod semnificativ prin pseudonimizarea adecvată a

angajaților și a clienților. Mai ales dacă cheile de pseudonimizare sunt rotite frecvent și se iau în considerare zone mari în locul adreselor detaliate, se realizează efectiv reducerea la minimum a datelor, iar operatorul se poate concentra exclusiv asupra procesului de livrare și asupra scopului de optimizare a resurselor, fără a depăși pragul de la care începe monitorizarea comportamentelor persoanelor fizice (clienți și angajați).

Exemplul 4

Un spital colectează date despre pacienții săi într-un sistem informatic spitalicesc (dosar electronic de sănătate). Personalul spitalului trebui să acceseze dosarele pacienților pentru a-și fundamenta deciziile privind îngrijirea și tratamentul acestora, precum și pentru a se documenta cu privire la toate acțiunile de diagnosticare, îngrijire și tratament întreprinse. În mod implicit, accesul este acordat doar membrilor personalului medical care s-au ocupat de tratamentul pacientului respectiv în cadrul secției de specialitate la care a fost trimis pacientul. Grupul de persoane care au acces la dosarul pacientului se mărește dacă în tratament se implică și alte secții sau unități de diagnosticare. După externarea pacientului și achitarea serviciilor, accesul se reduce la un grup redus de angajați din cadrul secției de specialitate, care răspund la solicitările de informații medicale sau la consultările efectuate sau solicitate de alți furnizori de servicii medicale autorizați în acest sens de către pacientul respectiv.

## 3.6 Exactitate

77. Datele cu caracter personal sunt exacte și actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere[38].

78. Cerințele trebuie privite în raport cu riscurile și consecințele utilizării concrete a datelor. Datele cu caracter personal inexacte pot constitui un risc pentru drepturile și libertățile persoanelor vizate, de exemplu atunci când generează un diagnostic eronat sau un tratament greșit în cadrul unui protocol sanitar sau o imagine incorectă a unei persoane poate genera luarea unor decizii pe un temei greșit, fie manual, folosind un proces decizional automatizat, fie prin inteligență artificială.

79. Exemple de elemente principale legate de concepere și de protecția implicită menite să asigure exactitatea:
    - Sursa de date - Sursele de date cu caracter personal trebuie să fie de încredere din punctul de vedere al exactității datelor.
    - Gradul de exactitate - Fiecare element de date cu caracter personal trebuie să fie exact, în măsura necesară în scopurile determinate.
    - Exactitatea măsurabilă - Reducerea numărului de rezultate fals pozitive/negative, de exemplu a rezultatelor distorsionate în cazul deciziilor automatizate și al inteligenței artificiale.
    - Verificarea - În funcție de natura datelor și în raport cu frecvența cu care se pot schimba acestea, operatorul trebuie să verifice cu persoana vizată corectitudinea datelor cu caracter personal înainte de prelucrare și în diferite etape ale acesteia (un exemplu sunt cerințele referitoare la vârstă).

[38] Articolul 5 alineatul (1) litera (d) din RGPD.

- Ștergerea/rectificarea - Operatorul trebuie să șteargă sau să rectifice datele inexacte fără întârziere. Operatorul trebuie să faciliteze acest lucru în special în cazul în care persoanele vizate sunt sau au fost copii și ulterior doresc să elimine datele respective cu caracter personal[39].
- Evitarea propagării erorilor - Operatorii trebuie să atenueze efectul unei erori acumulate în lanțul de prelucrare.
- Accesul - Persoanelor vizate trebuie să li se ofere informații cu privire la datele cu caracter personal și acces efectiv la acestea, în conformitate cu articolele 12 și 15 din RGPD, pentru a verifica exactitatea și a efectua rectificări în caz de necesitate.
- Exactitatea continuă - Datele cu caracter personal trebuie să fie exacte în toate etapele prelucrării, trebuind să se efectueze testări ale exactității în etapele critice.
- Actualizarea - Datele cu caracter personal trebuie să fie actualizate dacă este necesar în scopul respectiv.
- Conceperea datelor - Utilizarea unor configurații de proiectare tehnologică și organizatorică menite să reducă inexactitățile, de exemplu prezentarea unor opțiuni prestabilite clare în locul unor câmpuri de text liber.

Exemplul 1

O companie de asigurări dorește să utilizeze inteligența artificială (IA) pentru a crea profilul clienților care cumpără asigurări, care să stea la baza procesului de luare a deciziilor în urma calculării riscului de asigurare. În momentul în care stabilește modul în care trebuie să fie dezvoltate soluțiile de IA, compania stabilește mijloacele de prelucrare și trebuie să analizeze protecția datelor începând cu momentul conceperii atât atunci când alege o aplicație de inteligență artificială de la un furnizor, cât și atunci când decide modul în care va antrena respectiva inteligență artificială.

La determinarea modului de antrenare a IA, operatorul trebuie să dețină date exacte pentru a obține rezultate precise. Prin urmare, operatorul trebuie să se asigure că datele utilizate pentru antrenarea inteligenței artificiale sunt exacte.

Îndeplinind condiția de a deține un temei juridic valid pentru antrenarea inteligenței artificiale folosind date cu caracter personal dintr-un subansamblu mare de clienți existenți, operatorul alege un fond de clienți care este reprezentativ pentru populație, pentru a evita distorsionarea rezultatelor.

Se colectează apoi date referitoare la clienți din sistemul respectiv de gestionare a datelor, cuprinzând date privind tipul de asigurare, de exemplu asigurare de sănătate, asigurare pentru locuință, asigurare de călătorie etc., precum și din registrele publice la care operatorul are acces în mod legal. Toate datele sunt pseudonimizate înainte de a fi transferate în sistemul dedicat antrenării modelului de IA.

Pentru a se asigura că datele folosite la antrenarea IA sunt cât se poate de exacte, operatorul colectează date doar din surse cu informații corecte și actualizate.

Compania de asigurări testează dacă IA este fiabil și oferă rezultate nediscriminatorii atât în timpul dezvoltării produsului, cât și la final, înainte de lansarea acestuia. După ce inteligența artificială este pe deplin antrenată și operațională, compania de asigurări utilizează rezultatele pentru a sprijini evaluările riscului de asigurare, însă fără a se baza doar pe IA în decizia de încheiere a asigurării, cu

[39] Cf. considerentul 65.

excepția cazului în care decizia este luată în conformitate cu excepțiile de la articolul 22 alineatul (2) din RGPD.

De asemenea, compania de asigurări va revizui periodic rezultatele generate de IA, pentru a menține fiabilitatea algoritmului și a-l ajusta, după caz.

Exemplul 2

Operatorul este o instituție sanitară care caută metode prin care să asigure integritatea și exactitatea datelor cu caracter personal din registrele sale de clienți.

În situațiile în care la instituție sosesc simultan două persoane care primesc același tratament, există riscul de a le încurca dacă singurul parametru prin care se deosebesc cele două este numele. Pentru a asigura exactitatea, operatorul are nevoie de un cod unic de identificare pentru fiecare persoană și, prin urmare, de informații mai multe decât doar numele clientului.

Instituția folosește mai multe sisteme care conțin date cu caracter personal ale clienților și trebuie să se asigure că informațiile legate de client sunt corecte, exacte și consecvente în toate sistemele, în orice moment. Instituția a identificat mai multe riscuri care pot să apară dacă se schimbă informații într-unul dintre sisteme, dar nu și în celelalte.

Operatorul decide să atenueze riscul folosind o tehnologie de hashing care poate fi utilizată pentru a asigura integritatea datelor în jurnalul de tratament. Se creează marcaje temporale criptografice invariabile pentru înregistrările din jurnalul de tratament și pentru clientul asociat acestora, astfel încât orice modificări să poată fi recunoscute, corelate și urmărite dacă este necesar.

## 3.7 Limitări legate de stocare

80. Operatorul trebuie să se asigure că datele cu caracter personal sunt păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele[40].
Este vital ca operatorul să știe exact ce date cu caracter personal prelucrează compania și de ce. Scopul prelucrării este criteriul principal pentru a decide durata de stocare a datelor cu caracter personal.

81. Măsurile și garanțiile care pun în aplicare principiul limitărilor legate de stocare completează libertățile persoanelor vizate, în special dreptul la ștergerea datelor și dreptul la opoziție.

82. Exemple de elemente principale legate de concepere și de protecția implicită menite să asigure limitarea stocării:
    - Ștergerea și anonimizarea – Operatorul trebuie să aibă proceduri și funcționalități interne clare pentru ștergere și/sau anonimizare.
    - Eficacitatea anonimizării/ștergerii – Operatorul se asigură că nu este posibil să se reidentifice date anonimizate sau să se recupereze date șterse și trebuie să testeze dacă acest lucru este posibil.
    - Automatizarea – Ștergerea anumitor date cu caracter personal trebuie să fie automatizată.

[40] Articolul 5 alineatul (1) litera (c) din RGPD.

- Criteriile de stocare – Operatorul trebuie să determine datele și durata stocării care sunt necesare scopului.
- Justificarea – Operatorul trebuie să poată justifica motivul pentru care perioada de stocare este necesară scopului și datelor cu caracter personal în cauză și să poată divulga motivul, precum și temeiurile juridice pentru perioada de păstrare.
- Aplicarea politicilor de păstrare - Operatorul trebuie să aplice politici interne de păstrate și să desfășoare teste pentru a verifica dacă organizația își pune în practică politicile.
- Copiile de rezervă/jurnalele - Operatorii trebuie să determine ce date personale și ce durată de stocare sunt necesare pentru efectuarea copiilor de rezervă și a jurnalelor.
- Circulația datelor – Operatorii trebuie să evite circulația datelor cu caracter personal și stocarea de copii ale acestor date, precum și să încerce să limiteze stocarea lor „temporară”.

Exemplu

Operatorul colectează date cu caracter personal, scopul prelucrării fiind acela de a administra calitatea de membru a persoanei vizate. Datele cu caracter personal trebuie șterse atunci când calitatea de membru ia sfârșit și nu mai există un temei juridic pentru continuarea stocării lor.

În primul rând, operatorul întocmește o procedură internă pentru păstrarea și ștergerea datelor. Potrivit acesteia, angajații trebuie să șteargă manual datele cu caracter personal după ce se încheie perioada de păstrare. Angajatul urmează procedura potrivit căreia șterge și corectează în mod regulat datele de pe orice dispozitive, din copiile de rezervă, jurnale, e-mailuri și alte medii de stocare relevante.

Apoi, pentru ca ștergerea să fie mai eficace și mai puțin predispusă la erori, operatorul înlocuiește această procedură cu un sistem automat care să șteargă datele automat, în mod fiabil și la intervale mai regulate. Sistemul este configurat astfel încât să respecte o anumită procedură pentru ștergerea datelor, care are loc la intervale predefinite pentru a elimina date cu caracter personal din toate mediile de stocare ale companiei. Operatorul revizuiește și testează periodic procedura de păstrare și se asigură că aceasta este în concordanță cu politica de păstrare actualizată.

## 3.8 Integritate și confidențialitate

83. Principiul integrității și al confidențialității include protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice adecvate. Securitatea datelor cu caracter personal necesită măsuri adecvate, concepute pentru a preveni și gestiona incidentele de încălcare a securității datelor, pentru a garanta o execuție adecvată a sarcinilor de prelucrare a datelor, cu respectarea celorlalte principii, precum și pentru a facilita exercitarea efectivă a drepturilor persoanelor fizice.

84. Considerentul 78 afirmă că una dintre măsurile privind DPbDD poate consta în abilitarea operatorului *„să creeze elemente de siguranță și să le îmbunătățească”*. Alături de alte măsuri privind DPbDD, considerentul 78 sugerează o răspundere a operatorilor de a evalua în mod continuu dacă utilizează în permanență mijloace adecvate de prelucrare și de a evalua dacă măsurile alese combat în mod efectiv vulnerabilitățile existente. În plus, operatorii trebuie să efectueze revizuiri regulate ale măsurilor de securitate a informațiilor care înconjoară și protejează datele cu caracter personal, precum și ale procedurii de tratare a încălcării securității datelor.

85. Exemple de elemente principale legate de concepere și de protecția implicită menite să asigure integritatea și confidențialitatea:

- Sistemul de gestionare a securității informațiilor (ISMS) - Deținerea unui mijloc funcțional de gestionare a politicilor și procedurilor de securitate a informațiilor.
- Analiza riscurilor - Evaluarea riscurilor în raport cu securitatea datelor cu caracter personal, având în vedere impactul asupra drepturilor persoanelor fizice și combaterea riscurilor identificate. În vederea evaluării riscurilor, se elaborează și se menține o „modelare a amenințărilor" cuprinzătoare, sistematică și realistă și o analiză a suprafeței de atac a software-ului conceput, în vederea reducerii vectorilor de atac și a posibilităților de exploatare a punctelor slabe și a vulnerabilităților.
- Securitatea începând cu momentul conceperii – Luarea în considerare a cerințelor de securitate cât mai curând posibil în conceperea și dezvoltarea sistemului; integrarea și efectuarea în permanență a testelor relevante.
- Întreținerea – Revizuirea și testarea regulată a software-ului și a hardware-ului, a sistemelor și a serviciilor etc. pentru depistarea vulnerabilităților sistemului pe care are loc prelucrarea.
- Gestionarea controlului accesului – Doar personalul autorizat care are nevoie trebuie să aibă acces la datele cu caracter personal necesare pentru sarcinile sale de prelucrare, iar operatorul trebuie să facă diferența între privilegiile de acces ale personalului autorizat.
    - Limitarea accesului (agenți) – Configurarea prelucrării datelor astfel încât un număr minim de persoane să aibă nevoie de acces la datele cu caracter personal pentru a-și îndeplini sarcinile și limitarea accesului în consecință.
    - Limitarea accesului (conținut) – În contextul fiecărei operațiuni de prelucrare, accesul trebuie limitat numai la acele atribute ale fiecărui set de date care sunt necesare pentru a efectua operațiunea respectivă. Mai mult, accesul trebuie limitat la datele care aparțin persoanelor vizate de care se ocupă angajatul respectiv.
    - Separarea accesului – Configurarea prelucrării datelor astfel încât nicio persoană să nu aibă nevoie de acces cuprinzător la toate datele culese despre o persoană vizată, cu atât mai puțin la toate datele cu caracter personal ale unei categorii anume de persoane vizate.
- Transferurile securizate - Transferurile trebuie să fie securizate împotriva accesării și a modificării neautorizate și accidentale.
- Stocarea securizată - Stocarea datelor trebuie să fie securizată împotriva accesării și a modificării neautorizate. Trebuie să existe proceduri de evaluare a riscurilor stocării centralizate sau descentralizate, precum și de stabilire a categoriilor de date cu caracter personal cărora li se aplică aceasta. Este posibil ca unele date să necesite mai multe măsuri de securitate decât altele sau izolarea de alte date.
- Pseudonimizarea - Datele cu caracter personal și copiile de rezervă/ jurnalele trebuie să fie pseudonimizate ca măsură de siguranță pentru reducerea la minimum a riscurilor unor eventuale încălcări ale securității datelor, de exemplu folosind hashingul și criptarea.
- Copiile de rezervă/jurnalele - Menținerea unor copii de rezervă și a unor jurnale doar în măsura în care sunt necesare pentru securitatea informațiilor, utilizarea pistelor de audit și a monitorizării evenimentelor ca măsuri curente de control al securității. Acestea trebuie protejate de accesarea și modificarea neautorizate și accidentale și trebuie revizuite regulat, iar incidentele trebuie gestionate cu promptitudine.
- Recuperarea în caz de dezastru/continuitatea activității – Trebuie abordate cerințele de continuitate a activității și de recuperare în caz de dezastru a sistemului informatic pentru restabilirea disponibilității datelor cu caracter personal în urma incidentelor majore.

- Protecția în conformitate cu riscul – Toate categoriile de date cu caracter personal trebuie protejate cu măsuri adecvate riscului de încălcare a securității. Datele care prezintă riscuri speciale trebuie păstrate separat de restul datelor cu caracter personal dacă este posibil.
- Gestionarea răspunsului la incidentele de securitate - Punerea în practică a unor rutine, proceduri și resurse pentru a detecta, reduce, trata, raporta și învăța din incidentele de încălcare a securității datelor.
- Gestionarea incidentelor – Operatorul trebuie să aibă instituite procese de gestionare a încălcărilor și a incidentelor de securitate, pentru a consolida într-o măsură mai mare sistemul de prelucrare. Aceasta presupune proceduri de notificare, cum ar fi gestionarea notificării (autorității de supraveghere) și a informării (persoanelor vizate).

Exemplu

Un operator dorește să extragă volume mari de date cu caracter personal dintr-o bază de date medicală care conține dosare electronice de sănătate (ale pacienților) într-un server cu baze de date dedicat din cadrul companiei, pentru a prelucra datele extrase în scopul asigurării calității. Compania a evaluat că riscul redirecționării extraselor către un server accesibil tuturor angajaților companiei este probabil ridicat pentru drepturile și libertățile persoanelor vizate. Având în vedere că un singur departament din cadrul companiei are nevoie să prelucreze extrasele de date ale pacienților, operatorul decide să restricționeze accesul la serverul dedicat, acordându-l exclusiv angajaților din departamentul respectiv. În plus, pentru a reduce și mai mult riscurile, datele vor fi pseudonimizate înainte de a fi transferate.

Pentru a reglementa accesul și a reduce eventualele daune generate de malware, compania decide să separe rețeaua și să instituie măsuri de control al accesului la server. În plus, se realizează o monitorizare a securității și se implementează un sistem de detecție și prevenire a intruziunilor, izolat de utilizarea curentă. Se pune în aplicare un sistem de audit automat pentru a monitoriza accesul și modificările. Raportarea și alertele automate sunt generate din acesta dacă sunt configurate anumite evenimente legate de utilizare. Operatorul se va asigura că utilizatorii au acces numai în funcție de necesitatea de a cunoaște și în limitele nivelului de acces adecvat. Utilizarea necorespunzătoare poate fi depistată rapid și ușor.

Unele dintre extrase trebuie comparate cu noile extrase și, prin urmare, trebuie stocate pe o perioadă de trei luni. Operatorul decide să le includă în baze de date separate pe același server și să utilizeze o criptare transparentă și la nivel de coloană pentru stocarea lor. Cheile pentru decriptarea datelor la nivel de coloană sunt stocate în module de securitate dedicate care pot fi utilizate numai de personalul autorizat, însă nu pot fi extrase.

Gestionarea anticipată a incidentelor face ca sistemul să fie mai solid și mai fiabil. Operatorul înțelege că trebuie să fie încorporate măsuri și garanții preventive în întreaga activitate de prelucrare a datelor cu caracter personal pe care o întreprinde acum și în viitor și că, procedând în acest mod, poate contribui la prevenirea unor astfel de incidente de încălcare a securității datelor în viitor.

Operatorul instituie aceste măsuri de securitate atât pentru a asigura exactitatea, integritatea și confidențialitatea, cât și pentru a preveni răspândirea programelor malware prin atacuri cibernetice, precum și pentru a întări soluția adoptată. Măsurile de securitate solide contribuie la sporirea încrederii persoanelor vizate.

### 3.9 Responsabilitate[41]

86. Principiul responsabilității precizează că operatorul este responsabil cu respectarea tuturor principiilor menționate mai sus și trebuie să poată demonstra acest lucru.

87. Operatorul trebuie să poată demonstra respectarea principiilor. În acest scop, operatorul poate să demonstreze efectele măsurilor luate pentru a proteja drepturile persoanelor vizate, precum și motivul pentru care măsurile sunt considerate adecvate și eficace. De exemplu, se poate demonstra modul în care o măsură asigură cu adevărat respectarea principiului limitării legate de stocare.

88. Pentru a putea prelucra în mod responsabil datele cu caracter personal, operatorul trebuie să dețină atât cunoștințele, cât și capacitatea de a pune în aplicare protecția datelor. Acest lucru presupune ca operatorul să înțeleagă obligațiile care îi revin privind protecția datelor în baza RGPD și să poată să respecte obligațiile respective.

## 4 ARTICOLUL 25 ALINEATUL (3) CERTIFICAREA

89. În conformitate cu articolul 25 alineatul (3), certificarea în temeiul articolului 42 poate să fie utilizată drept element care să demonstreze conformitatea cu DPbDD. Este valabilă și reciproca: documentele care demonstrează respectarea DPbDD pot fi utile într-un proces de certificare. Aceasta înseamnă că, în cazul în care o operațiune de prelucrare efectuată de un operator sau de o persoană împuternicită de operator a fost certificată în baza articolului 42, autoritățile de supraveghere vor ține cont de acest lucru la evaluarea respectării RGPD, în mod special în ceea ce privește DPbDD.

90. Atunci când o operațiune de prelucrare efectuată de un operator sau de o persoană împuternicită de operator este certificată în conformitate cu articolul 42, elementele care contribuie la demonstrarea conformității cu articolul 25 alineatele (1) și (2) sunt procesele de concepere, adică procesul de stabilire a mijloacelor de prelucrare, guvernanța și măsurile tehnice și organizatorice de punere în aplicare a principiilor de protecție a datelor. Criteriile de certificare în domeniul protecției datelor sunt stabilite de organismele de certificare sau de deținătorii de sisteme de certificare, iar apoi sunt aprobate de autoritatea de supraveghere competentă sau de CEPD. Pentru informații suplimentare privind mecanismele de certificare, recomandăm cititorului să consulte Orientările CEPD privind certificarea[42] și alte orientări relevante publicate pe site-ul CEPD.

91. Chiar și atunci când unei operațiuni de prelucrare i se acordă o certificare în conformitate cu articolul 42, operatorul încă are responsabilitatea de a monitoriza și îmbunătăți continuu respectarea criteriilor DPbDD de la articolul 25.

## 5 APLICAREA ARTICOLULUI 25 ȘI CONSECINȚELE NERESPECTĂRII

92. Autoritățile de supraveghere pot să evalueze respectarea articolului 25 conform procedurilor enumerate la articolul 58. Competențele corective sunt specificate la articolul 58 alineatul (2) și includ emiterea de avertizări, mustrări, dispoziții de a respecta drepturile persoanelor vizate, impunerea de limitări sau interdicții asupra prelucrării, amenzi administrative etc.

[41] A se vedea considerentul 74, în baza căruia operatorii trebuie să demonstreze eficacitatea măsurilor adoptate.

[42] CEPD, „Orientările nr. 1/2018 privind certificarea și identificarea criteriilor de certificare în conformitate cu articolele 42 și 43 din Regulament”. Versiunea 3.0, 4 iunie 2019. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_ro

93. DPbDD este un factor suplimentar în determinarea nivelului sancțiunilor financiare pentru încălcarea RGPD – a se vedea articolul 83 alineatul (4)[43] [44].

# 6 RECOMANDĂRI

94. Deși nu sunt abordate direct la articolul 25, persoanele împuternicite de operator și producătorii sunt de asemenea recunoscuți ca factori determinanți esențiali pentru DPbDD, iar aceștia trebuie să știe că operatorii trebuie să prelucreze datele cu caracter personal numai cu sisteme și tehnologii care încorporează măsuri de protecție a datelor.

95. Atunci când prelucrează date în numele operatorilor sau când le furnizează soluții operatorilor, persoanele împuternicite de operator și producătorii trebuie să își utilizeze competențele pentru a genera încredere și pentru a-și îndruma clienții, inclusiv IMM-urile, în conceperea/achiziționarea unor soluții care să încorporeze protecția datelor în cadrul prelucrării. La rândul său, acest lucru înseamnă că produsele și serviciile trebuie concepute astfel încât să faciliteze nevoile operatorilor.

96. La punerea în aplicare a articolului 25, trebuie să se țină seama de faptul că principalul obiectiv în faza de concepere este *punerea în aplicare eficace* a principiilor și a *protecției* drepturilor persoanelor vizate în cadrul unor măsuri de prelucrare adecvate. Pentru a facilita și spori adoptarea DPbDD, facem următoarele recomandări pentru operatori, precum și pentru producători și persoanele împuternicite de operatori:

- Operatorii trebuie să se gândească la protecția datelor din *etapele inițiale* ale planificării unei operațiuni de prelucrare, chiar înainte de momentul determinării mijloacelor de prelucrare.

- În cazul în care operatorul are un responsabil cu protecția datelor (RPD), CEPD încurajează implicarea activă a RPD pentru integrarea DPbDD în procedurile de achiziție și dezvoltare, precum și în întregul ciclu al prelucrării.

- O operațiune de prelucrare poate să fie *certificată*. Capacitatea de a obține certificarea operațiunii de prelucrare conferă un plus de valoare operatorului atunci când trebuie să aleagă între diferite opțiuni de software, hardware, servicii și/sau sisteme de prelucrare de la producători sau persoane împuternicite de operatori. Prin urmare, producătorii trebuie să depună eforturi pentru a demonstra respectarea DPbDD în ciclul de elaborare a unei soluții de prelucrare. Existența unui sigiliu de certificare ar putea, de asemenea, să determine persoanele vizate să aleagă un anumit produs sau serviciu în detrimentul altuia. Capacitatea de a obține certificarea unei prelucrări poate să constituie un avantaj concurențial pentru producători, operatori și persoanele împuternicite de operatori și poate chiar să sporească încrederea persoanelor vizate în prelucrarea datelor lor cu caracter personal. În cazul în care nu se acordă nicio certificare, operatorii trebuie să caute să obțină alte *garanții* privind faptul că producătorii sau persoanele împuternicite de operatori respectă cerințele privind DPbDD.

[43] Articolul 83 alineatul (2) din RGPD prevede că, atunci când se determină impunerea amenzilor administrative pentru încălcarea RGPD, *se acordă „atenția cuvenită" în ceea ce privește „gradul de responsabilitate al operatorului sau al persoanei împuternicite de operator ținându-se seama de măsurile tehnice și organizatorice implementate de aceștia în temeiul articolelor 25 și 32".*

[44] Mai multe informații despre amenzi se găsesc în documentul Grupului de lucru „Articolul 29", „Orientări privind aplicarea și stabilirea unor amenzi administrative în sensul Regulamentului nr. 2016/679". WP 253, 3 octombrie 2017. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237 – aprobate de CEPD

- Operatorii, persoanele împuternicite de operatori și producătorii trebuie să aibă în vedere obligația de a acorda o protecție specială copiilor cu vârsta sub 18 ani și altor categorii vulnerabile, în conformitate cu DPbDD.

- Producătorii și persoanele împuternicite de operatori trebuie să urmărească să faciliteze punerea în aplicare a DPbDD pentru a sprijini capacitatea operatorului de a respecta obligațiile prevăzute la articolul 25. La rândul lor, operatorii nu trebuie să aleagă producători sau persoane împuternicite ale căror sisteme nu le permit sau nu îi ajută să respecte articolul 25, întrucât operatorii sunt cei care vor fi trași la răspundere pentru neîndeplinirea obligațiilor.

- Producătorii și persoanele împuternicite de operatori trebuie să joace un rol activ în asigurarea îndeplinirii criteriilor privind „stadiul actual al tehnologiei” și să notifice operatorii cu privire la orice modificări ale „stadiului actual al tehnologiei” care pot afecta eficacitatea măsurilor puse în aplicare. Operatorii trebuie să includă această cerință sub forma unei clauze contractuale pentru a se asigura că sunt informați.

- CEPD recomandă operatorilor să solicite producătorilor și persoanelor împuternicite de operatori să demonstreze în ce fel soluțiile hardware, software, serviciile sau sistemele îi permit operatorului să respecte cerințele privind responsabilitatea în conformitate cu DPbDD, de exemplu utilizând indicatori-cheie de performanță pentru a demonstra eficacitatea măsurilor și a garanțiilor instituite pentru respectarea principiilor și a drepturilor.

- CEPD subliniază necesitatea unei abordări armonizate pentru a pune în aplicare principiile și drepturile într-un mod eficace și încurajează asociațiile sau organismele care întocmesc coduri de conduită în conformitate cu articolul 40 să încorporeze și orientări privind DPbDD specifice fiecărui sector.

- Operatorii trebuie să dea dovadă de echitate față de persoanele vizate și de transparență privind modul în care evaluează și demonstrează punerea în aplicare eficace a DPbDD, în același mod în care operatorii demonstrează respectarea RGPD în temeiul principiului responsabilității.

- Tehnologiile de creștere a confidențialității (*privacy-enhancing technologies* – PET) care au ajuns la maturitate în stadiul actual al tehnologiei pot fi folosite ca reper în conformitate cu cerințele DPbDD, dacă este cazul, într-o abordare bazată pe risc. PET în sine nu îndeplinesc neapărat obligațiile prevăzute la articolul 25. Operatorii trebuie să evalueze dacă măsura este adecvată și eficace în punerea în aplicare a principiilor de protecție a datelor și a drepturilor persoanelor vizate.

- Sistemele deja existente se supun acelorași obligații privind DPbDD ca noile sisteme. Dacă sistemele existente nu respectă deja DPbDD și dacă nu pot fi modificate astfel încât să respecte obligațiile respective, sistemele existente pur și simplu nu îndeplinesc obligațiile prevăzute de RGPD și nu pot fi folosite pentru prelucrarea de date cu caracter personal.

- Articolul 25 nu impune un prag mai scăzut de respectare a cerințelor pentru IMM-uri. Următoarele idei pot facilita respectarea articolului 25 de către IMM-uri:

    - Efectuarea timpurie de evaluări ale riscurilor

    - Efectuarea inițială a unor operațiuni restrânse de prelucrare, apoi extinderea domeniului de aplicare și creșterea nivelului de complexitate

    - Căutarea unor garanții privind respectarea DPbDD de către producători și persoanele împuternicite de operatori, cum ar fi certificarea sau respectarea unor coduri de conduită

    - Alegerea unor parteneri cu istoric bun

    - Discutarea cu autoritățile de protecție a datelor (APD)

    - Consultarea orientărilor realizate de APD și de CEPD

    - Respectarea codurilor de conduită, după caz

    - Obținerea de ajutor specializat și consultanță

Pentru Comitetul european pentru protecția datelor

Președinte

(Andrea Jelinek)