Ce este Legea nr. 195/2024 privind protecția datelor cu caracter personal

Legea nr. 195/2024 privind protecția datelor cu caracter personal transpune *Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE*.

Persoanele fizice sau juridice, autoritățile publice, agențiile sau alte organisme care, singure sau împreună cu altele, stabilesc scopurile și mijloacele de prelucrare a datelor cu caracter personal se numesc **operatori**.

Datele cu caracter personal ale **persoanelor fizice vizate** trebuie să fie protejate de către operatori prin măsuri adecvate împotriva dezvăluirilor către terți și împotriva utilizării lor nelegale.

Legea nr. 195/2024 consacră principiul **responsabilității**, potrivit căruia, operatorul de date are obligația de a implementa măsuri tehnice și organizatorice adecvate pentru asigurarea protecției datelor cu caracter personal. Aceasta înseamnă că, *operatorului îi revine sarcina de a proba conformitatea, respectiv, obligația de a demonstra că aceste măsuri au fost efectiv adoptate și aplicate*.

În consecință, nu este suficientă simpla asigurare a protecției datelor cu caracter personal, ci se impune și documentarea corespunzătoare a proceselor de prelucrare, prin elaborarea și menținerea unor politici și proceduri adecvate, inclusiv registre de evidență a activităților de prelucrare, analize de risc, acorduri cu partenerii contractuali/persoanele contractante, consimțăminte valabil exprimate și documentate, precum și informări adresate persoanelor vizate.

Principiile de prelucrare

Legea nr. 195/2024 introduce **șapte principii-cheie care trebuie respectate** de către orice operator care prelucrează datele cu caracter personal (art. 5).
Aceste principii sunt: *(1) legalitatea, echitatea și transparența*; *(2) limitarea scopului; (3) reducerea la minim a datelor; (4) exactitatea; (5) limitările legate de stocare; (6) integritate și confidențialitate; (7) responsabilitate.*

Principiul legalității, echității și transparenței

Principiul legalității, *echității și transparenței* presupune faptul că datele cu caracter personal trebuie prelucrate în mod legal, echitabil și transparent față de persoana vizată.
Prelucrarea legală a datelor cu caracter personal înseamnă că datele trebuie să fie prelucrate în conformitate cu legea și să se încadreze cel puțin în unul dintre temeiurile juridice de prelucrare de la art. 6 din Legea nr. 195/2024. Aceste temeiuri sunt consimțământul, contractul, obligația legală, interesul vital, interesul public și interesul legitim. În situația în care prelucrarea datelor nu respectă legea atunci prelucrarea va fi ilegală, iar operatorul riscă aplicarea unei amenzi. În mod similar, dacă prelucrarea datelor nu se bazează pe niciun temei juridic dintre cele prevăzute la art. 6 din Legea nr. 195/2024 atunci prelucrarea datelor cu caracter personal va fi ilegală.
Legalitatea prelucrării categoriilor speciale de date cu caracter personal trebuie să respecte anumite cerințe suplimentare. Categoriilor speciale de date cu caracter personal sunt datele cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice; datele privind apartenența la sindicate, datele genetice, datele biometrice în vederea identificării unei ființe umane, datele cu privire la sănătate, datele privind viața sexuală sau orientarea sexuală a unei persoane. Prelucrarea acestor date este, în general, interzisă. Cu toate acestea, există situații când prelucrarea lor este legală (art. 9), de exemplu atunci când datele sunt necesare pentru încheierea unui contract de muncă sau pentru furnizarea unor servicii medicale.

Principiul echității înseamnă faptul că datele cu caracter personal nu pot fi prelucrate în moduri incorecte, imorale sau în moduri care ar putea prejudicia persoanele vizate.

Principiul transparenței înseamnă faptul că persoanele fizice trebuie să cunoască modul în care un operator îi prelucrează datele (art. 12). Astfel, pentru a respecta principiul transparenței, operatorii trebuie să informeze persoana vizată cu privire la modul în care îi prelucrează datele. Această informare trebuie, de regulă, să se facă înainte de colectarea datelor. Informarea se realizează prin intermediul unor note de informare. Principiul transparenței presupune și faptul că operatorii trebuie să comunice în mod optim și transparent cu persoanele vizate și să le faciliteze exercitarea drepturilor.

Principiul limitării scopului

Scopurile prelucrării datelor trebuie să fie determinate, explicite și legitime. Legea nr. 195/2024 interzice ca datele cu caracter personal să fie prelucrate în alte scopuri incompatibile cu scopurile inițiale. De exemplu, dacă inițial o companie a colectat numărul de telefon al unui client pentru a-i putea livra un produs comandat, ultimul nu poate utiliza acest număr de telefon într-un scop incompatibil. Astfel, dacă în viitor, această companie își extinde obiectul de activitate pentru a organiza evenimente, nu poate utiliza numărul de telefon al clientului pentru a-l invita la eveniment. Acest scop (invitarea la eveniment) este diferit și incompatibil de scopul inițial (livrarea bunurilor). Fiind un scop incompatibil, prelucrarea datelor cu caracter personal în noul scop nu va putea fi bazată, spre exemplu, pe consimțământul acordat inițial și, astfel, va fi ilegală.

Principiul reducerii la minimum a datelor

Principiul reducerii la minimum a datelor presupune faptul că operatorii trebuie să prelucreze doar cantitatea minimă de date pentru atingerea scopului stabilit. Operatorii nu au voie să prelucreze mai multe date decât le trebuie. Cu alte cuvinte, în materie de date cu caracter personal - „*ce e prea mult, strică*”. De exemplu, pentru livrarea unui produs, o companie are nevoie de numele, adresa, telefonul și (eventual) adresa de e-mail a clientului. Prelucrarea altor date care nu ar fi necesară atingerii scopului (livrarea bunurilor) va fi ilegală. De exemplu, prelucrarea IDNP-ului, a imaginii faciale sau a datei de naștere va fi, în general, ilegală deoarece s-ar încălca principiul „*reducerii la minimum a datelor*”.

Principiul exactității

Principiul exactității înseamnă că datele cu caracter personal trebuie să fie exacte, complete și actualizate. Pentru a respecta acest principiu, companiile trebuie să depună toate eforturile pentru a verifica dacă datele cu caracter personal sunt actualizate. Datele care sunt inexacte trebuie șterse sau actualizate fără întârziere.

Principiul integrității și confidențialității

Pentru a respecta acest principiu, operatorul trebuie, în primul rând, să asigure securitatea datelor. De exemplu, operatorul trebuie să protejeze datele împotriva accesărilor neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale. Conform Legii nr. 195/2024, pentru a asigura integritatea și confidențialitatea datelor cu caracter personal, operatorul trebuie să

ia măsuri tehnice și organizatorice adecvate, de exemplu, să implementeze politici și proceduri de protecție a datelor cu caracter personal.

Principiul responsabilității

Principiul responsabilității înseamnă faptul că operatorul este responsabil cu privire la respectarea principiilor de mai sus și că poate demonstra această conformitate. Cu alte cuvinte, principiul responsabilității înseamnă nu doar că operatorul trebuie să respecte principiile Legii nr. 195/2024, ci și faptul că el trebuie să fie capabil să demonstreze că respectă aceste principii. Demonstrarea respectării principiilor se realizează, de exemplu, prin implementarea unor politici și proceduri de protecție a datelor cu caracter personal.

Temeiurile legale

Toate operațiunile asupra datelor cu caracter personal trebuie să fie legale, adică să se bazeze pe cel puțin unul dintre temeiurile de mai jos (art. 6):

- ***Consimțământul*** *– persoana și-a dat în mod valabil consimțământul;*
- ***Contractul*** *– există un contract sau urmează să se încheie un contract;*
- ***Obligația legală*** *– există o obligație/prevedere legală;*
- ***Interesul vital*** *– pentru a proteja viața sau sănătatea persoanei;*
- ***Interesul public -*** *îndeplinirea unei sarcini efectuate în interes public sau în exercitarea competenței unei autorități publice;*
- ***Interesul legitim*** *– atâta timp cât nu intră în conflict cu interesul persoanei fizice.*

Indiferent de temei (consimțământul, contractul, obligația legală etc), operatorul trebuie să respecte Legea nr. 195/2024 și să pună în practică politici adecvate de protecție a datelor.

Cele șase temeiuri enumerate mai sus se află pe poziție de **egalitate**.
Consimțământul este important, însă el vine cu dezavantaje, cum ar fi, dreptul de retragere a consimțământului, imposibilitatea de a obține consimțământul tuturor persoanelor, refuzul de a oferi consimțământul. De aceea, operatorul trebuie să verifice dacă poate prelucra datele în baza altui temei. *Dacă există o obligație legală sau un contract cu persoana* nu este nevoie de consimțământ.

Consimțământul persoanei trebuie să îndeplinească o serie de condiții, printre care să fie **cert și informat.** Căsuțele pre-bifate, tăcerea sau inacțiunea nu se echivalează cu oferirea unui consimțământ. **Persoana trebuie să își dea consimțământul printr-o acțiune reală, precum bifarea unei căsuțe, o semnătură sau un „DA" categoric înregistrat.**

Consimțământul trebuie să fie însoțit de o notă de informare prin care persoana să afle **pentru ce anume își dă consimțământul.**

Operatorul va trebui să poată demonstra că a obținut consimțământul valabil și să îi permită persoanei să își retragă în orice moment consimțământul la fel de simplu cum l-a dat, dar nu neapărat prin aceeași acțiune.

Pentru copii sub 16 ani, își vor da părinții consimțământul. Iar în anumite cazuri, precum prelucrarea datelor sensibile sau transferul internațional de date, consimțământul trebuie să fie **explicit:** verificare în doi factori, semnătură scrisă, semnătură electronica etc. În ceea ce privește oferirea de servicii ale societății informaționale direct unui copil, prelucrarea datelor cu caracter personal ale unui copil în baza consimțământului va fi considerată legală dacă copilul are cel puțin vârsta de 14 ani. În cazul copilului cu vârsta sub 14 ani, respectiva prelucrare este legală numai dacă și în măsura în care consimțământul respectiv este acordat sau autorizat de reprezentantul legal al copilului.

Interesul legitim se va folosi cu precauție. El se folosește, de regulă, pentru situații în care nu există, nu se poate sau nu se dorește obținerea consimțământului și nu există alt temei (supraveghere video, monitorizare locație gps, recrutare, organizări evenimente etc). Pentru a se putea utiliza interesul legitim, este nevoie ca operatorul să documenteze în scris că interesul său primează asupra drepturilor și intereselor persoanelor vizate.

Ce drepturi are persoana fizică?

Legea nr. 195/2024 oferă persoanei fizice mai multe drepturi. Persoana vizată își poate exercita aceste drepturi în raport cu operatorul de date, prin transmiterea unei cereri în acest sens. De exemplu, persoana vizată își poate exercita dreptul la ștergerea datelor prin transmiterea unei cereri de ștergere a datelor către operator. Operatorul nu poate ignora aceasta cerere. El trebuie să o înregistreze și să răspundă în termen legal. Acest termen expiră la o lună de la primirea cererii. Dacă cererea este complexă sau dacă operatorul are prea multe cereri, termenul de o lună poate fi prelungit cu încă două luni. Operatorul informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând și motivele întârzierii.

Mai jos se va prezenta o descriere a drepturilor persoanei vizate:

Dreptul la informare *(art. 13 – art. 14) - persoana trebuie să fie informată, cu privire la ce date sunt prelucrate, de ce, în ce scopuri, cui sunt transmise și ce drepturi are;*

Dreptul de acces la date *(art. 15) - persoana are dreptul de acces la datele cu caracter personal colectate care o privesc și trebuie să își exercite acest drept cu ușurință și la intervale de timp rezonabile, pentru a fi informată cu privire la prelucrare și pentru a verifica legalitatea acesteia.*

Dreptul la rectificare *(art. 16) - persoana are dreptul de a obține rectificarea datelor incomplete și inexacte care o privesc;*

Dreptul la ștergerea datelor *(art. 17) - în unele situații, persoana are dreptul de a obține din partea operatorului ștergerea, fără întârzieri nejustificate, a datelor cu caracter personal care o privesc, iar operatorul are obligația de a șterge datele cu caracter personal fără întârzieri nejustificate;*

Dreptul la restricționarea prelucrării *(art. 18 – art. 19) - în unele cazuri, persoana fizică are dreptul de a solicita și obține restricționarea datelor cu caracter personal;*

Dreptul la portabilitatea datelor *(art. 20) - în unele cazuri, persoana fizică are dreptul de a solicita și obține portabilitatea datelor cu caracter personal;*

Dreptul la opoziție *(art. 21) - dreptul persoanei de a se opune prelucrării, atunci când există temei;*

Dreptul de a nu fi supus unei decizii automate, inclusiv crearea de profiluri *(art. 22)* ***-*** *persoana are dreptul de a nu fi supusă unei decizii automate cu impact semnificativ. În situația în care este supusă acestei decizii, ea are dreptul de a o contesta și dreptul de a solicita intervenție umană.*

Responsabilul cu protecția datelor

Conform Legii nr. 195/2024, desemnarea responsabilului cu protecția datelor este obligatorie în anumite cazuri (art. 37 - art. 39). Deși desemnarea nu are caracter imperativ, aceasta este recomandabilă, având în vedere rolul esențial al responsabilului în asigurarea conformității cu dispozițiile legale privind protecția datelor cu caracter personal.

Responsabilul cu protecția datelor este un specialist/expert în domeniul legislației privind protecția datelor, care sprijină operatorul în special pe următoarele paliere:

- *monitorizarea respectării cadrului normativ aplicabil;*
- *gestionarea relației cu persoanele vizate;*
- *asigurarea legăturii și cooperării cu autoritatea de supraveghere competentă.*

Desemnarea responsabilului cu protecția datelor este obligatorie în următoarele situații:

- *atunci când operatorul este o autoritate sau un organism public;*
- *atunci când activitățile principale ale operatorului constau în operațiuni de monitorizare periodică și sistematică a persoanelor vizate pe scară largă;*
- *atunci când activitățile principale ale operatorului constau în prelucrarea pe scară largă a unor categorii speciale de date (art. 9 alin. (1)) sau date cu caracter personal referitoare la condamnări penale și infracțiuni (art. 10).*

Responsabilul cu protecția datelor poate fi desemnat și în alte cazuri decât cele prevăzute supra, sau, atunci când actele normative impun acest lucru.

Responsabilul cu protecția datelor are atribuția de a monitoriza respectarea dispozițiilor Legii nr. 195/2024 de către operator și îndeplinește rolul de principal punct de contact atât în relația cu CNPDCP, cât și în relația cu persoanele vizate.
Funcția de responsabil cu protecția datelor are caracter independent. În exercitarea atribuțiilor sale legale, acesta nu poate fi sancționat sau revocat din funcție pentru îndeplinirea cu bună-credință a obligațiilor ce îi revin în materia monitorizării conformității cu dispozițiile legale aplicabile.

Evidența activităților de prelucrare

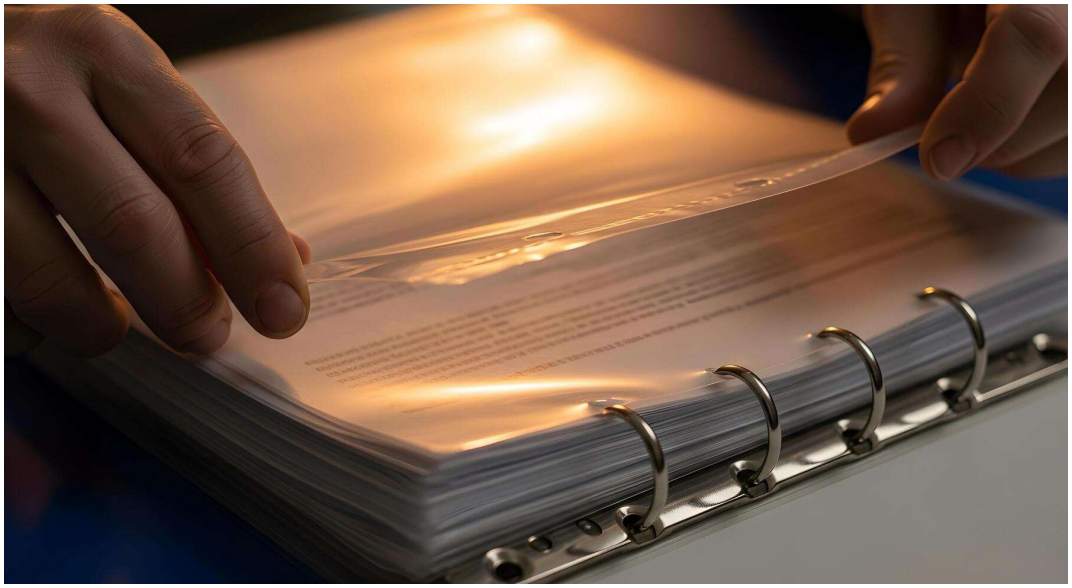
Potrivit Legii nr. 195/2024 (art. 30), operatorii și persoanele împuternicite de operator au obligația de a ține o evidență a activităților de prelucrare, în următoarele situații:

• atunci când entitatea are mai mult de 250 angajați;
• atunci când prelucrarea este susceptibilă să genereze un risc pentru drepturile și libertățile persoanei vizate;
• atunci când prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date (art. 9 alin. (1)) sau date cu caracter personal referitoare la condamnări penale și infracțiuni (art. 10).

În practică, având în vedere că, în mod obișnuit, activitățile de prelucrare desfășurate în cadrul unei companiei nu au caracter ocazional, rezultă că, în majoritatea cazurilor, operatorii au obligația de a institui și menține o evidență internă a activităților de prelucrare, care să fie actualizată și revizuită periodic.

Evidența activităților de prelucrare poate fi organizată, spre exemplu, sub forma unui registru și trebuie să cuprindă, cel puțin, următoarele informații:
• numele și datele de contact ale operatorului;
• scopurile prelucrării;
• categoriile de date prelucrate;
• categoriile de persoane vizate;
• categoriile de destinatari;
• transferurile de date către alte state, dacă e cazul;
• termenele-limită preconizate pentru ștergerea diferitelor categorii de date, dacă este posibil;
• o descriere generală a măsurilor tehnice și organizatorice de securitate luate, dacă este posibil.

Această evidență constituie un instrument esențial pentru demonstrarea conformității operatorului cu obligațiile legale în materia protecției datelor cu caracter personal.



Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit

Legea nr. 195/2024 instituie două noi principii esențiale pentru operatori (art. 25):

Privacy by desing – atunci când se dezvoltă aplicații care vor prelucra date cu caracter personal trebuie să se asigure, încă din stadiul dezvoltării, că aplicația va respecta regulile stabilite de Legea nr. 195/2024.

Privacy by default – atunci când operatorul furnizează o aplicație care prelucrează date personale trebuie să se asigure că setările inițiale le vor permite utilizatorilor să își mențină controlul asupra vieții private, asupra a ceea ce postează sau împărtășesc cu alți utilizatori.

Evaluarea impactului asupra protecției datelor

Evaluarea impactului asupra protecției datelor (art. 35) este obligatorie atunci când prelucrarea poate genera un risc ridicat pentru drepturile persoanelor, în special în cazuri precum:

- *profilare sau decizii automate cu efecte juridice;*
- *prelucrarea pe scară largă a datelor sensibile (sănătate, date biometrice, opinii politice etc.);*
- *monitorizare video sau supraveghere sistematică a spațiilor publice;*
- *monitorizarea minorilor sau a angajaților;*
- *utilizarea unor tehnologii noi (ex. recunoaștere facială);*
- *utilizarea pe scară largă a dispozitivelor inteligente (IT);*
- *prelucrarea sistematică a datelor de localizare sau trafic.*

O listă detaliată este aprobată de CNPDCP.

Evaluarea impactului trebuie să includă cel puțin:

- *descrierea prelucrării și a scopului acesteia;*
- *analiza necesității și proporționalității;*
- *evaluarea riscurilor pentru persoanele vizate;*
- *măsurile luate pentru reducerea riscurilor și asigurarea conformității.*

Operatorul consultă CNPDCP înainte de prelucrare atunci când evaluarea impactului asupra protecției datelor cu caracter personal indică faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri luate de operator pentru atenuarea riscului.

Evaluarea impactului trebuie realizată înainte de începerea prelucrării și cât mai devreme în etapa de planificare. Este un proces continuu și trebuie actualizată atunci când apar modificări semnificative ale prelucrării. **Totodată, o evaluare a impactului va fi realizată și pentru sistemele sau operațiunile de prelucrare deja existente și funcționale**, susceptibile să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice prin însăși natura lor, prin domeniul lor de aplicare, prin contextul și prin scopurile lor, **în situația în care o evaluare a impactului asupra protecției datelor nu a fost efectuată anterior de către operator**.

Securitatea datelor

Operatorii și persoanele împuternicite trebuie să ia măsuri tehnice și organizatorice adecvate pentru a proteja datele personale, în funcție de riscurile existente (art. 32).

Aceste măsuri pot include:

- criptarea sau pseudonimizarea datelor;
- protejarea confidențialității, integrității și disponibilității sistemelor;
- posibilitatea de a restaura rapid datele în caz de incident;
- testarea periodică a măsurilor de securitate.

Angajații pot prelucra datele doar conform instrucțiunilor primite, iar respectarea unor coduri de conduită sau certificări poate ajuta la demonstrarea conformității.

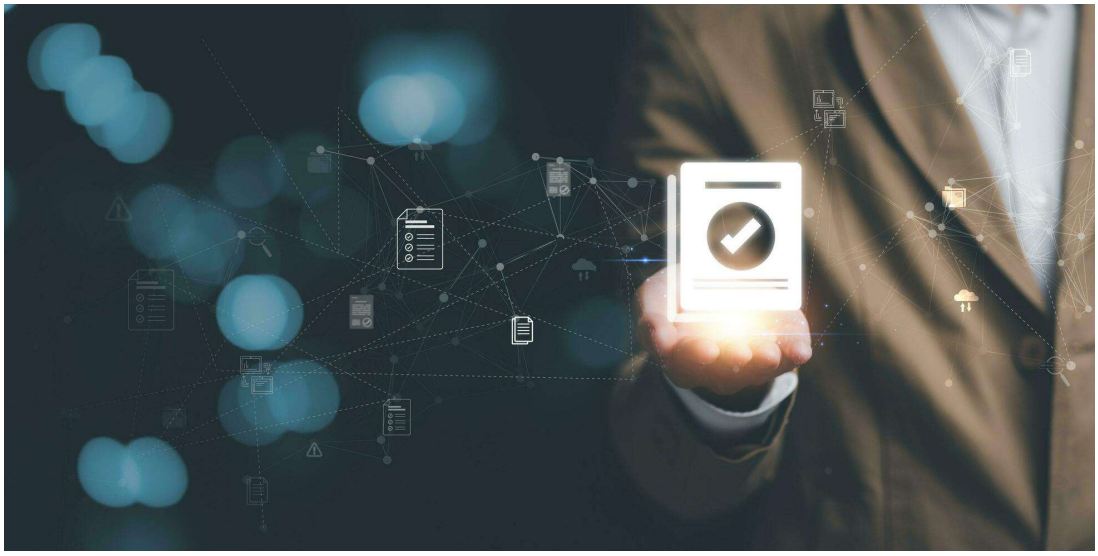
O încălcare a securității (breșă) poate duce la distrugerea, pierderea, modificarea sau divulgarea neautorizată a datelor cu caracter personal ori la accesul neautorizat la acestea.

O astfel de situație poate produce prejudicii persoanelor vizate, precum furt de identitate, fraudă, pierderi financiare sau afectarea reputației.

Legea nr. 195/2024 obligă operatorul să notifice CNPDCP în cel mult 72 de ore de la momentul în care a luat cunoștință de încălcare, dacă există un risc pentru drepturile și libertățile persoanelor (art. 33).

Operatorul are obligația să documenteze toate breșele, inclusiv cauzele, efectele și măsurile luate pentru remediere.

În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare (art. 34).

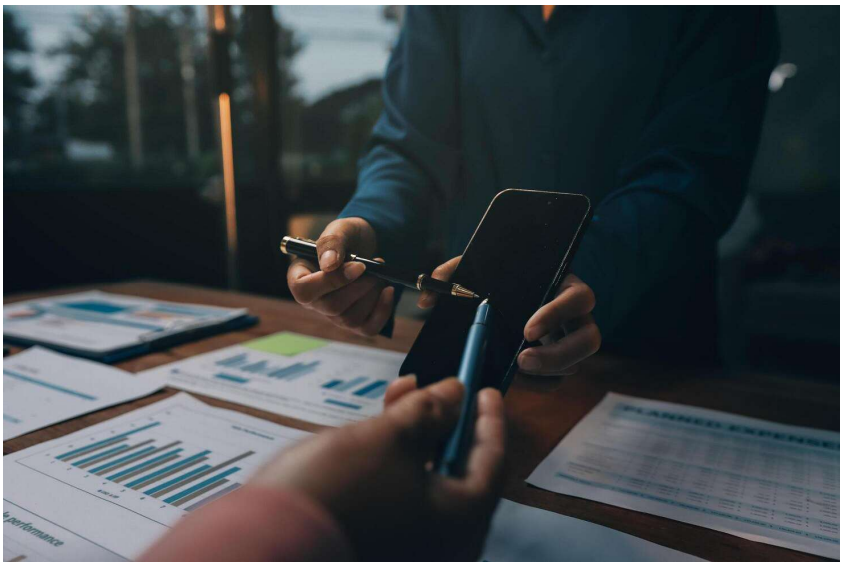


Transmiterea datelor cu caracter personal și asigurarea existenței garanțiilor de conformitate

În situația în care se transmit date cu caracter personal între doi operatori, în temeiul Legii nr. 195/2024, operatorul care transmite datele trebuie să se asigure că destinatarul oferă garanții suficiente privind implementarea unor măsuri tehnice și organizatorice adecvate pentru protecția datelor cu caracter personal.

Transmiterea datelor trebuie realizată în condiții de securitate, cu respectarea principiilor legalității, echității, transparenței, integrității și confidențialității. Datele cu caracter personal pot fi comunicate exclusiv către parteneri (alți operatori sau persoane împuternicite) care demonstrează un nivel adecvat de conformitate cu normele privind protecția datelor. În consecință, operatorul nu poate iniția sau continua relații contractuale care implică prelucrarea de date cu caracter personal cu entități ce nu prezintă garanții suficiente în acest sens.

Anterior încheierii unui contract care implică transmiterea sau accesul la date cu caracter personal, operatorul ar trebui să efectueze o evaluare prealabilă (audit de conformitate) a potențialului partener, în vederea verificării nivelului de protecție a datelor asigurat de acesta. Evaluarea poate include analiza politicilor interne, a procedurilor de securitate, a măsurilor tehnice implementate, precum și a istoricului privind incidentele de securitate.



În ipoteza în care, în urma evaluării, se constată că potențialul partener nu oferă garanții suficiente pentru asigurarea protecției datelor cu caracter personal, operatorul are obligația de a se abține de la transmiterea datelor. Încălcarea acestei obligații, prin transmiterea datelor către o entitate care nu oferă/asigură suficiente garanții de protecție a datelor cu caracter personal, poate atrage răspunderea și aplicarea sancțiunilor prevăzute de Legea nr. 195/2024.

Pentru asigurarea unei conformități continue, este recomandabil ca operatorul să efectueze evaluări/auditări periodice ale partenerilor săi, cel puțin anual sau ori de câte ori intervin modificări relevante în activitatea acestora. Evaluarea/auditarea poate fi realizată prin completarea unor chestionare de conformitate, solicitarea de documente justificative sau, în situații care implică volume semnificative de date ori categorii speciale de date cu caracter personal, prin audituri tehnice aprofundate (de exemplu, evaluarea infrastructurii IT, testări de securitate, teste de penetrare sau verificarea mecanismelor de criptare și control al accesului).

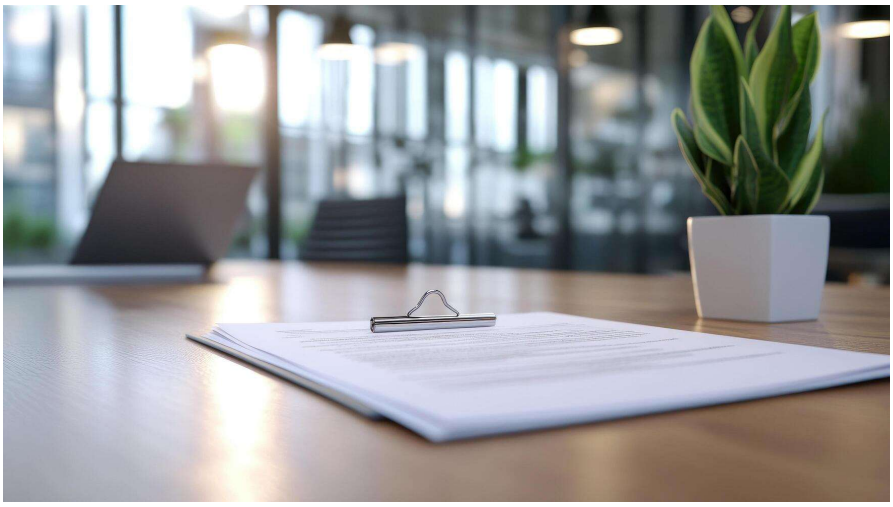
Adoptarea unei astfel de proceduri contribuie la demonstrarea respectării principiului responsabilității și la diminuarea riscului juridic asociat prelucrării și transmiterii datelor cu caracter personal.

Acordurile între operator și persoana împuternicită

Legea nr. 195/2024 este foarte clară cu referire la faptul că trebuie să existe acorduri/contracte scrise între operator și persoana împuternicită, care are acces la date, și stabilește ce anume trebuie să conțină acestea. De exemplu, operatorul trebuie să aibă contracte semnate cu alte companii către care transmite date (firme de contabilitate, IT, HR, marketing, etc).

Împuternicitul trebuie să respecte termeni clari în materie de protecție a datelor, iar contractele existente trebuie actualizate cu acorduri de prelucrare. Chiar și în situația în care, pentru activitatea desfășurată între părți, nu a fost încheiat un contract în formă scrisă, Legea nr. 195/2024 impune obligativitatea încheierii unui contract sau a unui alt act juridic în formă scrisă care să reglementeze prelucrarea datelor cu caracter personal aferentă activității desfășurate.

Astfel, în materia protecției datelor, existența unui instrument juridic scris între operator și persoana împuternicită nu este opțională, ci reprezintă o cerință legală expresă, menită să stabilească în mod clar obiectul, durata, natura și scopul prelucrării, precum și drepturile și obligațiile părților.



Transferurile de date către alte state sau organizații internaționale

Transferul de date ale cetățenilor către alte state și organizații internaționale ridică întrebări despre cât de bine pot fi protejate aceste date (art. 44 - art. 50).

Legea nr. 195/2024 nu interzice în mod expres transferurile de date, ci precizează că acestea pot avea loc dacă există garanții corespunzătoare, de exemplu:

- *Decizii adecvate.*
- *Reguli corporatiste obligatorii;*
- *Clauze standard.*

Există și derogări pentru situații specifice, cum ar fi consimțământul explicit al persoanei sau necesitatea executării unui contract.

Centrul Național pentru Protecția Datelor cu Caracter Personal (CNPDCP)

CNPDCP este autoritatea de supraveghere independentă responsabilă, printre altele, de monitorizarea respectării legislației în materie de protecție a datelor, efectuarea investigațiilor, aplicarea sancțiunilor și sprijinul persoanelor vizate.

Căi de atac, răspundere și sancțiuni

Legea nr. 195/2024 prevede faptul că amenda poate ajunge în cuantum de până la 2.000.000 de lei sau, în cazul unei întreprinderi, de până la 2% din cifra totală de afaceri (art. 88).

Atunci când optează între a aplica un avertisment sau o amendă și cuantumul acesteia, CNPDCP ia în calcul mai mulți factori printre care: gradul de conformare, măsurile implementate, gravitatea abaterii, numărul încălcărilor, prejudiciile aduse persoanelor vizate și acțiunile întreprinse de operator sau de persoana împuternicită de operator pentru a reduce prejudiciul suferit de persoana vizată (art. 87).

Persoanele vizate nemulțumite de modul în care un operator le prelucrează datele au dreptul de a depune o plângere la CNPDCP și de a se adresa instanțelor de judecată pentru obținerea despăgubirilor (art. 74).