REGULAMENTUL nr. 679 din 27 aprilie 2016

Privind protecția prelucrării datelor cu caracter personal și privind libera circulație a acestor date

(RGPD

Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul General privind Protecția Datelor) urmează să fie pus direct în aplicare în toate statele membre ale Uniunii Europene începând ***cu data de 25 mai 2018***.

Un element de noutate pe care acest act normativ european îl aduce în peisajul juridic românesc și reprezintă instituirea obligativității desemnării la nivelul operatorului sau persoanei împuternicite de operator, în anumite cazuri, a unui **responsabil cu protecția datelor**.

Pentru asigurarea unei aplicări unitare a Regulamentului General privind Protecția Datelor, Grupul de Lucru Art. 29 de pe lângă Comisia Europeană a emis **Ghidul privind Responsabilul cu protecția datelor (DPO)**, accesibil la secțiunea specială dedicată Regulamentului General privind Protecția Datelor, la dresa http:// www.dataprotection.ro /servlet/ViewDocument?id=1384, accesibilă pe site-ul Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal.

GENERALITĂȚI

Prelucrarea datelor cu caracter personal ar trebui să fie în serviciul cetăţenilor. Dreptul la protecţia datelor cu caracter personal nu este un drept absolut; acesta trebuie luat în considerare în raport cu funcţia pe care o îndeplineşte în societate şi echilibrat cu alte drepturi fundamentale, în conformitate cu principiul proporţionalităţii.

Prezentul regulament respectă toate drepturile fundamentale şi libertăţile şi principiile recunoscute în cartă astfel cum sunt consacrate în tratate, în special respectarea vieţii private şi de familie, a reşedinţei şi a comunicaţiilor, a protecţiei datelor cu caracter personal, a libertăţii de gândire, de conştiinţă şi de religie, a libertăţii de exprimare şi de informare, a libertăţii de a desfăşura o activitate comercială, dreptul la o cale de atac eficientă şi la un proces echitabil, precum şi diversitatea culturală, religioasă şi lingvistică.

CONTEXT

Parlamentul European și Consiliul au adoptat, în data de 27.aprilie 2016, regulamentul (UE) 2016/679, 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 95/469/CE (Regulamentul general privind Protecția datelor-RGPD).

Regulamentul (UE) 2016/679 impune un set unic de reguli în materia protecției datelor cu caracter personal, înlocuind Directiva 95/46/CE și implicit prederile Legii nr. 677/2001.

NOUTĂȚI:

Regulamentul (UE) 2016/679 pune accent pe transparența față de persoana vizată și responsabilizarea operatorului de date față de modul în care prelucrează datele cu caracter personal.

Prezentul regulament stabilește o serie de garanții specifice pentru a proteja cât mai eficient viața privată a minorilor, în special în mediul on-line.

Domeniul de aplicare:

RGPD se aplică:

Prelucrării datelor cu caracter personal în cadrul activităților derulate la sediul unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii.

RGPD - NU se aplică prelucrării datelor cu caracter personal:

(a) în cadrul unei activități care nu intră sub incidența dreptului Uniunii;

(b) de către statele membre, atunci când desfășoară activități care intră sub incidența capitolului 2 al titlului V din Tratatul UE;

(c) de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice;

(d) de către autorități competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau al executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora.

PRINCIPALELE OBLIGAȚII PENTRU OPERATORII DE DATE ÎN APLICAREA RGPD

Pentru a îndruma modul în care sunt gestionate datele cu caracter personal în cadrul unui operator sau al unei persoane împuternicite de operator în anumite situații, este necesară existența unei persoane care să exercite o misiune de informare, de consiliere și de control în plan intern: **responsabilul cu protecția datelor.**

Desemnarea unui responsabil cu protecția datelor este obligatorie **din 25 mai 2018,** raportat la dispozițiile art. 37-39 din regulamentul General privind Protecția datelor, în cazul în care operatorul sau persoana împuternicită de operator:

- este o autoritate publică sau organism public excepție instanțelor jurisdicționale;

- desfășoară o activitate principală care conduce la monitorizarea constantă și sistematică a persoanelor.

- desfășoară activități constând în prelucrarea datelor pe scară largă (ex. date privind originea rasială, etnică, convingeri religioase, sindicale, date genetice, biometrice, și privind strarea de sănătate).

Rolul responsabilului cu protecția datelor:

- să informeze și să consilieze operatorul sau poersoana împuternicită de operator, precum și angajații acestora cu privire la obligațiile existente în domeniul protecției datelor cu caracter personal.

- să monitorizeze respectarea RGPD și a legislației naționale în domeniul protecției datelor;

- să consilieze operatorul sau persoana împuternicită în legătură cu realizarea de studii de impact privind protecția datelor și să verifice efectuarea acestora;

- să coopereze cu autoritatea pentru protecția datelor și să reprezinte punctul de contact în relația cu aceasta.

Când nu este necesară desemnarea unui responsabil cu protecţia datelor?

- atunci când nu se prelucrează pe scară largă date cu caracter personal.

Spre exemplu:

- prelucrarea datelor pacientului de către un cabinet medical individual;

- prelucrarea datelor personale referitoare la condamnările penale și infracțiuni de către un cabinet individual de avocatură.

De reținut!

Deși în unele cazuri nu este necesară desemnarea unui responsabil cu protecția datelor, Autoritatea de Supraveghere recomandă numirea unei astfel de persoane, întrucât este utilă operatorului pentru respectarea obligațiilor în domeniul protecției datelor cu caracter personal.

Domeniul de aplicare material :

(1) Prezentul regulament se aplică prelucrării datelor cu caracter personal, efectuată total sau parţial prin mijloace automatizate, precum şi prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidenţă a datelor sau care sunt destinate să facă parte dintr-un sistem de evidenţă a datelor.

(2) Prezentul regulament nu se aplică prelucrării datelor cu caracter personal:

a) în cadrul unei activităţi care nu intră sub incidenţa dreptului Uniunii;

b) de către statele membre atunci când desfăşoară activităţi care intră sub incidenţa capitolului 2 al titlului V din Tratatul UE;

c) de către o persoană fizică în cadrul unei activităţi exclusiv personale sau domestice;

d) de către autorităţile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracţiunilor, sau al executării sancţiunilor penale, inclusiv al protejării împotriva ameninţărilor la adresa siguranţei publice şi a prevenirii acestora.

(3) Pentru prelucrarea datelor cu caracter personal de către instituţiile, organele, oficiile şi agenţiile Uniunii, se aplică Regulamentul (CE) nr. 45/2001. Regulamentul (CE) nr. 45/2001 şi alte acte juridice ale Uniunii aplicabile unei asemenea prelucrări a datelor cu caracter personal se adaptează la principiile şi normele din prezentul regulament, în conformitate cu articolul 98.

Art. 3: Domeniul de aplicare teritorial :

(1) Prezentul regulament se aplică prelucrării datelor cu caracter personal în cadrul activităţilor unui sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii.

(2) Prezentul regulament se aplică prelucrării datelor cu caracter personal ale unor persoane vizate care se află în Uniune de către un operator sau o persoană împuternicită de operator care nu este stabilit(ă) în Uniune, atunci când activităţile de prelucrare sunt legate de:

a) oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăţi de către persoana vizată; sau

b) monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Uniunii.

(3) Prezentul regulament se aplică prelucrării datelor cu caracter personal de către un operator care nu este stabilit în Uniune, ci într-un loc în care dreptul intern se aplică în temeiul dreptului internaţional public.

Cine poate îndeplini funcția de responsabil cu protecția datelor?

Articolul 37 alin. 5 din Regulamentul UE 2016/679 stabilește ca responsabilul cu protecția datelor să fie ”desemnat pe baza calităţilor profesionale şi, în special, a cunoştinţelor de specialitate în dreptul şi practicile din domeniul protecţiei datelor, precum şi pe baza capacităţii de a îndeplini sarcinile prevăzute la articolul 39.”

Responsabilul cu protecția datelor

- în domeniul public

- în domeniul privat, raportat la situațiile prevăzute expres de art. 37 RGDP.

Responsabilul cu protecția datelor poate fi angajat al operatorului/persoanei împuternicite de operator sau poate să-și îndeplinească sarcinile pe baza unui contract de prestări servicii.

În domeniul public, poate fi **desemnat pentru mai multe autorități sau instituții publice**, luând în considerare structura organizatorică și dimensiunea acestora.

Definiţii

În sensul prezentului regulament:

1."date cu caracter personal " - orice informaţie privind o persoană fizică identificată sau identificabilă ("persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

2."prelucrare" - orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea;

3. " restricţionarea prelucrării" - marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

4. "creare de profiluri" - orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanţa la locul de muncă, situaţia economică, sănătatea, preferinţele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia;

5. "pseudonimizare" - prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea ***să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informaţii suplimentare,*** cu condiţia ca aceste informaţii suplimentare să fie stocate separat şi să facă obiectul unor măsuri de natură tehnică şi organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;

6."sistem de evidenţă a datelor" - orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcţionale sau geografice;

7."operator" - persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;

8. "persoană împuternicită de operator" - persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

9. "destinatar" - persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terţă. Cu toate acestea, autorităţile publice cărora li se pot comunica date cu character personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autorităţile publice respective respectă normele aplicabile în materie de protecţie a datelor, în conformitate cu scopurile prelucrării;

10. **"parte terţă"** - o persoană fizică sau juridică, autoritate publică, agenţie sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator şi persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

11. **"consimţământ al persoanei vizate"** - orice manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declaraţie sau printr-o acţiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

12. **"încălcarea securităţii datelor cu caracter personal"** - o încălcare a securităţii care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;

13. **"date genetice"** - datele cu caracter personal referitoare la caracteristicile genetice moştenite sau dobândite ale unei persoane fizice, care oferă informaţii unice privind fiziologia sau sănătatea persoanei respective şi care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;

14. **"date biometrice"** - o dată cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;

15. **"date privind sănătatea"** - date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistenţă medicală, care dezvăluie informaţii despre starea de sănătate a acesteia;

Principii

Art. 5: Principii legate de prelucrarea datelor cu caracter personal

(1)Datele cu caracter personal sunt:

a) prelucrate în mod legal, echitabil şi transparent faţă de persoana vizată ("legalitate, echitate şi transparenţă");

b) colectate în scopuri determinate, explicite şi legitime şi nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile iniţiale, în conformitate cu articolul 89 alineatul (1) ("limitări legate de scop");

c) adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate ("reducerea la minimum a datelor");

d) exacte şi, în cazul în care este necesar, să fie 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 şterse sau rectificate fără întârziere ("exactitate");

e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depăşeşte perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), sub rezerva punerii în aplicare a măsurilor de ordin tehnic şi organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor şi libertăţilor persoanei vizate ("limitări legate de stocare");

f) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecţia împotriva prelucrării neautorizate sau ilegale şi împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare ("integritate şi confidenţialitate").

Art. 6: Legalitatea prelucrării:

(1) Prelucrarea este legală numai dacă şi în măsura în care se aplică cel puţin una dintre următoarele condiţii:

a) persoana vizată şi-a dat consimţământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;

b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;

c) prelucrarea este necesară în vederea îndeplinirii unei obligaţii legale care îi revine operatorului; *Să fie folosite numai formulare prev. de legile în vigoare (*pe fiecare document "să fie menţionat prevederea legală";*

d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;

e) prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul;

f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terţă, cu excepţia cazului în care prevalează interesele sau drepturile şi libertăţile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

Litera (f) din primul paragraf nu se aplică în cazul prelucrării efectuate de autorităţi publice în îndeplinirea atribuţiilor lor.

Art. 7: Condiţii privind consimţământul:

(1) În cazul în care prelucrarea se bazează pe consimţământ, operatorul trebuie să fie în măsură să demonstreze că persoana vizată şi-a dat consimţământul pentru prelucrarea datelor sale cu caracter personal.

(2) În cazul în care consimţământul persoanei vizate este dat în contextul unei declaraţii scrise care se referă şi la alte aspecte, cererea privind consimţământul trebuie să fie prezentată într-o formă care o diferenţiază în mod clar de celelalte aspecte, într-o formă inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu. Nicio parte a respectivei declaraţii care constituie o încălcare a prezentului regulament nu este obligatorie.

(3) Persoana vizată are dreptul să îşi retragă în orice moment consimţământul. Retragerea consimţământului nu afectează legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia. Înainte de acordarea consimţământului, persoana vizată este informată cu privire la acest lucru. Retragerea consimţământului se face la fel de simplu ca acordarea acestuia.

(4) Atunci când se evaluează dacă consimţământul este dat în mod liber, se ţine seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiţionată sau nu de consimţământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract.

Notă: „*se interzice prezentarea unui tipizat persoanei vizate în vederea semnării privind acordarea consimțământului pentru prelucrarea datelor cu caracter personal”*.

Exemple de situații care pot constitui o monitorizare periodică și sistematică a persoanelor vizate:

- gestionarea unei rețele de telecomunicații;
- profilare și scoring în scopul evaluării riscurilor (de exemplu, în scopul acordării unui credit, stabilirea primelor de asigurare, de prevenire a fraudelor, detectarea spălării banilor);
- urmărirea locației, spre exemplu prin aplicații mobile (geolocalizare);
- desfășurarea de programe de loialitate;
- monitorizarea stării de sănătate prin intermediul dispozitivelor portabile;
- televiziune cu circuit închis - CCTV;
- prelucrarea datelor pacienților de către un spital;
- prelucrarea datelor datelor de conținut, locație, trafic de către furnizorii de servicii de internet;
- prelucrarea datelor personale de către companii de asigurări;
- publicitate comportamentală.

Calități și competențe:

Trebuie să aibă capacitatea de a îndeplini sarcinile. În acest sens sunt necesare anumite calități personale (ex: integritate și etică profesională), cunoștințe, dar și o anumită poziție în cadrul organizației.

Trebuie să aibă anumite calități profesionale, astfel:

- experiență în legislația și practicile de protecție a datelor la nivel național și european, precum și o înțelegere adecvată a RGPD;

- nivelul necesar de cunoștințe în domeniul protecției datelor în funcție de operațiunile de prelucrare a datelor efectuate și de nivelul de protecție necesar pentru datele cu caracter personal prelucrate;

- să înțeleagă operațiunile de prelucrare efectuate, precum și sistemele de informații și necesitățile de securitate și protecție a datelor prelucrate de operator;

-în cazul unei autorități sau instituții publice, responsabilul cu protecția datelor trebuie să dețină, de asemenea, cunoștințe privind reglementările legale referitoare la organizarea și funcționarea acestora, precum și a procedurilor interne administrative ce vizează desfășurarea activității.

Prelucrarea de categorii speciale de date cu caracter personal

Se interzice prelucrarea de date cu caracter personal din categoria celor speciale.

Categoriile de date personale speciale sunt acele date cu caracter personal care dezvăluie :

- originea rasială* sau *etnică;

- opiniile politice;

- confesiunea religioasă sau convingerile filozofice;

- apartenența la sindicate;

- prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice;

- date privind sănătatea;

- date privind viața sexuală sau orientarea sexuală ale unei persoane fizice.

A. Informaţii care se furnizează în cazul în care datele cu caracter personal sunt colectate de la persoana vizată :

(1) În cazul în care datele cu caracter personal referitoare la o persoană vizată sunt colectate de la aceasta, operatorul, în momentul obţinerii acestor date cu caracter personal, furnizează persoanei vizate toate informaţiile următoare:

a) identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acestuia;

b) datele de contact ale responsabilului cu protecţia datelor, după caz;

c) scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării;

d) în cazul în care prelucrarea se face în temeiul articolului 6 alineatul (1) litera (f), interesele legitime urmărite de operator sau de o parte terţă;

e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal;

f) dacă este cazul, intenţia operatorului de a transfera date cu caracter personal către o ţară terţă sau o organizaţie internaţională şi existenţa sau absenţa unei decizii a Comisiei privind caracterul adecvat sau, în cazul transferurilor menţionate la articolul 46 sau 47 sau la articolul 49 alineatul (1) al doilea paragraf, o trimitere la garanţiile adecvate sau corespunzătoare şi la mijloacele de a obţine o copie a acestora, în cazul în care acestea au fost puse la dispoziţie.

B. Informaţii care se furnizează în cazul în care datele cu caracter personal nu au fost obţinute de la persoana vizată:

(1) În cazul în care datele cu caracter personal nu au fost obţinute de la persoana vizată, operatorul furnizează persoanei vizate următoarele informaţii:

a) identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acestuia;

b) datele de contact ale responsabilului cu protecţia datelor, după caz;

c) scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării;

d) categoriile de date cu caracter personal vizate;

e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz;

f) dacă este cazul, intenţia operatorului de a transfera date cu caracter personal către un destinatar dintr-o ţară terţă sau o organizaţie internaţională şi existenţa sau absenţa unei decizii a Comisiei privind caracterul adecvat sau, în cazul transferurilor menţionate la articolul 46 sau 47 sau la articolul 49 alineatul (1) al doilea paragraf, o trimitere la garanţiile adecvate sau corespunzătoare şi la mijloacele de a obţine o copie a acestora, în cazul în care acestea au fost puse la dispoziţie.

Art. 24: Responsabilitatea operatorului

(1) Ţinând seama de natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi de riscurile cu grade diferite de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice, **operatorul pune în aplicare măsuri tehnice şi organizatorice adecvate pentru a garanta şi a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament.** Respectivele măsuri se revizuiesc şi se actualizează dacă este necesar.

Persoana împuternicită de operator nu recrutează o altă persoană împuternicită de operator fără a primi în prealabil o autorizație scrisă sau specifică sau generală din partea operatorului.

Operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura că în mod implicit sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării. În special astfel de măsuri asigură că, în mod implicit, DCP nu pot fi accesate fără intervenția persoanei de un număr nelimitat de persoane.

OBLIGAȚIILE OPERATORULUI:

- Obligația, în anumite condiții, de desemnare a unui responsabil cu protecția datelor (DPO)
- Obligația de a formula politicile de confidențialitate și celelelte mijloace de informare într-un limbaj clar și ușor de înțeles pentru persoanele vizate.
- Obligația de obținere a consimțământului persoanerlor vizate în vederea prelucrării datelor acestora.
- Obligația de a informa persoanele vizate cu privire la scopurile prelucrării, datele care sunt prelucrate și drepturile pe care acestea le au.
- Obligația de a pune în aplicare măsurile tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prevederile regulamentului.
- Obligația de a asigura cartografierea prelucrărilor de DCP.
- Obligația de a notifica breșele de securitate cu privire la datele personale.

IMPLEMENTAREA GDPR:

- **Identificare de acțiuni** care trebuie întreprinse pentru conformarea la cerințele impuse de GDPR.
- **Prioritizare** în funcție de riscurile pe care le prezintă prelucrările efectuate pentru drepturile și libertățile persoanelor vizate.

Se vor avea în vedere:

- Colectarea și prelucrarea doar a datelor strict necesare pentru realizarea scopurilor;
- Identificarea temeiului legal în baza căruia se efectuează prelucrarea;
- Revizuirea/completarea informațiilor furnizate persoanelor vizate;
- Asigurarea că persoanele împuternicite își cunosc noile obligații și responsabilități;
- Verificarea existenței clauzelor contractuale și actualizarea obligațiilor persoanelor împuternicite privind securitatea, confidențialitatea și protecția datelor cu caracter presonal (PDCP), prelucrate;
- Stabilirea modalităților de executare a drepturilor persoanelor vizate (ex. dreptul de acces, dreptul de rectificare, dreptul la portabilitate, retragerea consimțământului)

Evidenţele activităţilor de prelucrare:

(1) Fiecare operator şi, după caz, reprezentantul acestuia păstrează o evidenţă a activităţilor de prelucrare desfăşurate sub responsabilitatea lor. Respectiva evidenţă cuprinde toate următoarele informaţii:

a) numele şi datele de contact ale operatorului şi, după caz, ale operatorului asociat, ale reprezentantului operatorului şi ale responsabilului cu protecţia datelor;

b) scopurile prelucrării;

c) o descriere a categoriilor de persoane vizate şi a categoriilor de date cu caracter personal;

d) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din ţări terţe sau organizaţii internaţionale;

e) dacă este cazul, transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, inclusiv identificarea ţării terţe sau a organizaţiei internaţionale respective şi, în cazul transferurilor menţionate la articolul 49 alineatul (1) al doilea paragraf, documentaţia care dovedeşte existenţa unor garanţii adecvate;

f) acolo unde este posibil, termenele-limită preconizate pentru ştergerea diferitelor categorii de date;

g) acolo unde este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate menţionate la articolul 32 alineatul (1).

Securitatea – DCP:

Art. 32: Securitatea prelucrării

(1) Având în vedere stadiul actual al dezvoltării, costurile implementării şi natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi riscul cu diferite grade de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice, operatorul şi persoana împuternicită de acesta implementează măsuri tehnice şi organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:

a) pseudonimizarea şi criptarea datelor cu caracter personal;

b) capacitatea de a asigura confidenţialitatea, integritatea, disponibilitatea şi rezistenţa continue ale sistemelor şi serviciilor de prelucrare;

c) capacitatea de a restabili disponibilitatea datelor cu caracter personal şi accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;

d) un proces pentru testarea, evaluarea şi aprecierea periodice ale eficacităţii măsurilor tehnice şi organizatorice pentru a garanta securitatea prelucrării.

(2) La evaluarea nivelului adecvat de securitate, se ţine seama, în special, de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

(3) Aderarea la un cod de conduită aprobat, menţionat la articolul 40, sau la un mecanism de certificare aprobat, menţionat la articolul 42.

(4) Operatorul şi persoana împuternicită de acesta iau măsuri pentru a asigura faptul că orice persoană fizică care acţionează sub autoritatea operatorului sau a persoanei împuternicite de operator şi care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepţia cazului în care această obligaţie îi revine în temeiul dreptului Uniunii sau al dreptului intern.

Securitatea – DCP:

Art. 33: Notificarea autorității în cazul încălcării securității DCP:

(1) În cazul în care are loc o încălcare a securităţii datelor cu caracter personal, *operatorul* notifică acest lucru autorităţii de supraveghere competente, în termen de cel mult 72 de ore de la data la care a luat cunoştinţă de aceasta, cu excepţia cazului în care este susceptibilă să genereze un risc pentru drepturile şi libertăţile persoanelor fizice. *În cazul în care notificarea nu are loc în termen de 72 de ore, aceasta este însoţită de o explicaţie motivată din partea autorităţii de supraveghere în cazul în care.*

(2) Persoana împuternicită de operator are obligația să înștiințeaze operatorul fără întârzieri nejustificate cu privire la încălcare a securităţii datelor cu caracter personal.

(3) Operatorul păstrează documente referitoare la toate cazurile de încălcare a securităţii datelor cu caracter personal, care cuprind o descriere a situaţiei de fapt în care a avut loc încălcarea securităţii datelor cu caracter personal, a efectelor acesteia şi a măsurilor de remediere întreprinse. Această documentaţie permite autorităţii de supraveghere să verifice conformitatea cu prezentul articol.

Notificarea conține conform alin 1, cel puțin:

a) Descrierea incidentului, caracterul încălcării;

b) Categoriile și numărul aproximativ al persoanelor vizate;

c) Categoriile și numărul aproximativ al înregistrărilor în cauză**;**

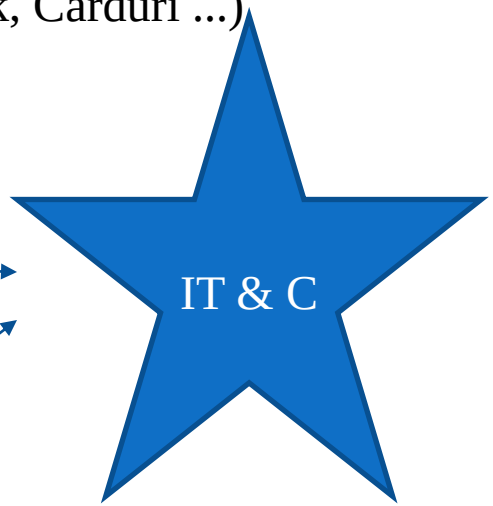
d) Descrierea consecințelor probabile ale încălcării;

e) Numele și datele de contact ale DPO sau un alt punct de contact de unde se pot obţine mai multe informaţii;

f) Descrierea măsurile luate sau propuse spre a fi luate de operator pentru rezolvarea problemei și a efectelor negative.

Sub ce formă exista DCP ?

- Hârtie (documente imprimate, dosare etc...)
- Electronic (HDD, CD, imagini video, Memory stick, Carduri ...)
- Know-how (resurse umane)



-Sistem informatic
(suport electronic)

-Sistem informațional
Hârtie, Know-how (resurse umane)

Securitatea datelor cu caracter personal

Atributele securității DCP:

Confidențialitatea

- Proprietatea informației **de a nu fi disponibilă** sau **diseminată entităților** care nu sunt **autorizate să aibă acces la aceastea**

Integritatea

- **Prorietatea informației de a-și păstra acuratețea și completitudinea**

Disponibilitatea

- **Proprietatea informației de a fi accesibilă și utilizabilă la cerere de către o entitate autorizată**

Rezistența continuă

- **Mecanismele de securitate fizică și informatică trebuie să reziste în cadrul unui atac ce ar viza obținerea/captarea/deteriorarea/distrugerea DCP (datelor cu caracter personal)**