

PROTECTIA DATELOR CU CARACTER PERSONAL

POTRIVIT REGULAMENTULUI GENERAL PENTRU PROTECTIA DATELOR (UE) 2016/679

Scopul : sa cunosc spiritul RGPD (regulamentul general pentru protectia datelor)

Regulamentul (UE) 2016/679 al Parlamentului European si al Consiliului European din 27 aprilie 2016 privind protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal si privind libera circulatie a acestor date si de abrogare a Directivei 95/46/CE (Regulament General privind Protectia Datelor - RGPD)

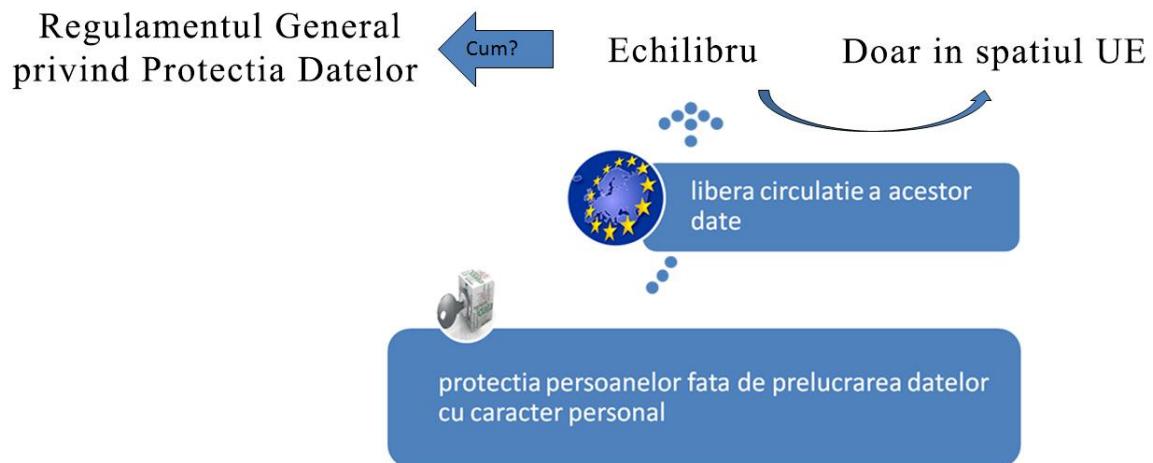
REGULAMENT

Regulamentul are aplicabilitate generala. Acesta este obligatoriu in toate elementele sale si se aplica direct in fiecare stat membru.

Regulamentul este un act legislativ cu caracter obligatoriu. Trebuie aplicat in integralitatea sa, in toate statele membre.

Directiva este obligatorie pentru fiecare stat membru destinatar cu privire la rezultatul care trebuie atins, lasand autoritatilor nationale competenta in ceea ce priveste forma si mijloacele.

Protectia datelor cu caracter personal



Protectia datelor cu caracter personal in cadrul entitatii



Regulamentul Protectia Datelor



REGULAMENTUL (UE) 2016/679

Datele cu caracter personal reprezinta orice informatie privind o persoana fizica identificata sau identificabila.



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 (IP), sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.

Operator:

Persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care singur sau împreună cu altele :

1. stabilește scopurile;
2. mijloacele de prelucrare a datelor cu caracter personal.

Atunci când scopurile și 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 .

Legalitatea prelucrarilor datelor cu caracter personal

Regulamentul UE 2016/679 (art.6)

- a) consumămantul persoanei vizate
- b) executarea unui contract
- c) obligație legală a operatorului
- d) interes vital
- e) interes public sau prerogative de autoritate
- f) interes legitim / proporțional cu interesul persoanei vizate

Principiile prelucrarii

Legea nr.677/2001

Datele cu caracter personal trebuie sa fie:

- colectate in scopuri determinate, explicite si legitime

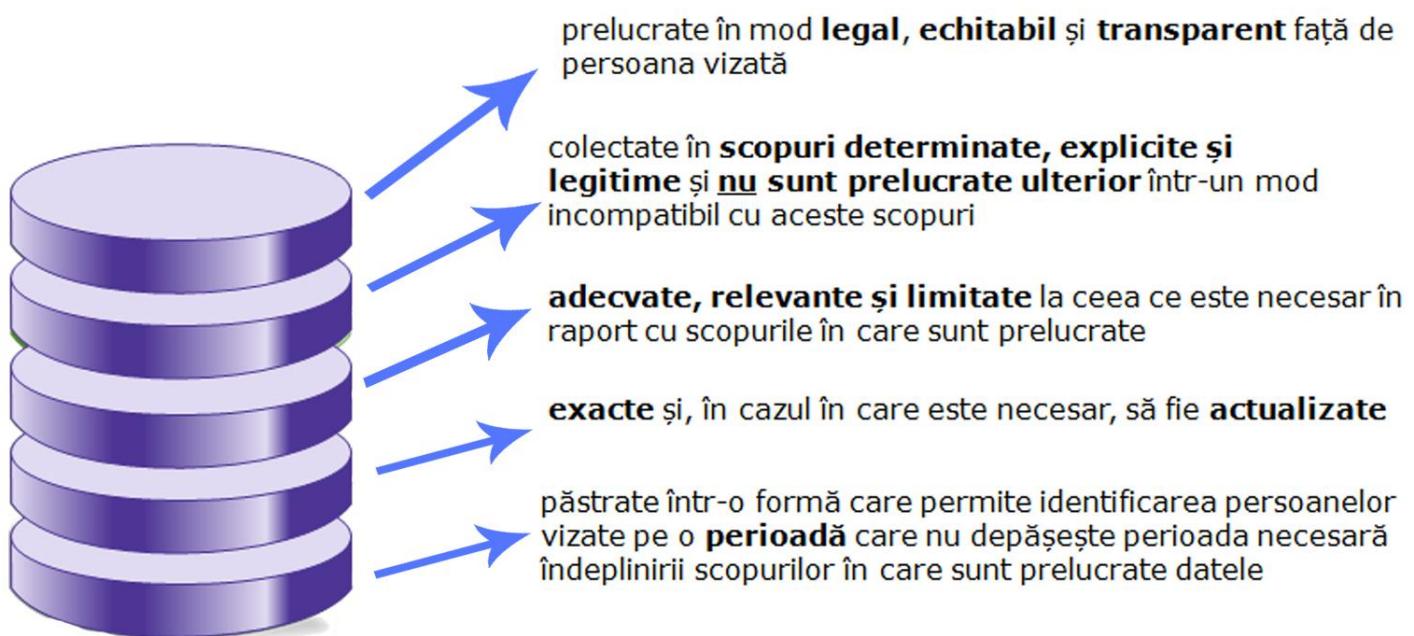
Directiva 95/46/CE

Datele cu caracter personal trebuie sa fie:

- colectate în scopuri determinate, explicite și legitime și să nu mai fie prelucrate ulterior într-un mod incompatibil cu aceste scopuri.

Regulamentul (UE) 2016/679

Principiile prelucrării



Prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare.

Regulamentul (UE) 2016/679

Principiile prelucrării

Legal, echitabil și transparent („legalitate, echitate și transparență”)
Scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior
„limitări legate de scop”)

Adequate, relevante și limitate („reducerea la minimum a datelor”)
Exacte și actualizate („exactitate”)
Perioadă de păstrare limitată („limitări legate de stocare”)
Securitatea adecvată („integritate și confidențialitate”)
Operatorul este responsabil de respectarea principiilor și
poate demonstra această respectare („responsabilitate”).

Principiile prelucrării (limitări legate de scop)

Regulamentul UE 2016/679 (art.5 lit.b)

Datele cu caracter personal sunt:

Colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri.

Prelucrarea ulterioară în scopuri privilegiate (arhivare în interes public, cercetare istorică sau științifică ori în scopuri statistice) nu este considerată incompatibilă (garanții instituite potrivit art.89).

Legalitatea prelucrarii

Regulamentul UE 2016/679 (art.6)

Consimtamantul persoanei vizate - executarea unui contract
Obligatie legala a operatorului - interes vital - interes public sau
prerogative de autoritate publică - Interes legitim.

Nu se poate baza pe :

- 1) Consimtamantul persoanei vizate dispozitie legala
- 2) Trebuie să se bazeze pe același temei juridic ca și prelucrarea initială
- 3) Scopuri privilegiate

Elemente de compatibilitate (art.6 alin.4)

- 1) Orice legătură dintre scopuri;
- 2) Contextul în care datele cu caracter personal au fost colectate, în special în ceea ce privește relația dintre persoanele vizate și operator;
- 3) Natura datelor cu caracter personal, în special în cazul prelucrării unor categorii speciale de date;
- 4) Posibilele consecințe asupra persoanelor vizate ale prelucrării ulterioare preconizate;
- 5) Existența unor garanții adecvate, care pot include criptarea sau pseudonimizarea.

Regulamentul (UE) 2016/679

Consimțământul

Operatorul trebuie să fie în măsură să demonstreze că persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal

Consimțământul trebuie să fie prezentat într-o formă care diferențiază în mod clar de celealte aspecte, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu.

Inainte de acordarea consimțământului, persoana vizată este informată cu privire la acest lucru.

Persoana vizată are dreptul să își retragă în orice moment consimțământul. Retragerea consimțământului se face la fel de simplu ca acordarea acestuia.

Consimțământul este dat în mod liber.

Se ține seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiționată sau nu de consimțământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract.

Categorii speciale de date cu caracter personal

Date cu caracter personal care dezvăluie

Originea rasială sau etnică / opiniile politice / confesiunea religioasă sau convingerile filozofice / apartenența la sindicate / prelucrarea de date genetice / date biometrice pentru identificarea unică a unei persoane fizice / date privind sănătatea / date privind viața sexuală, orientarea sexuală ale unei persoane fizice.

Conformitatea cu Regulamentul (UE) 2016/679

ETAPE:

1. Conștientizare;
2. Audit : identificarea prelucrărilor de date / inventarul datelor / identificarea fluxurilor de date / separarea fluxurilor funcționale / administrative;
3. Identificarea politicilor: procedurilor interne și reevaluare / determinarea responsabilităților / imputerniciti / destinatari / alți operatori;
4. Determinarea / stabilirea bazei legale pentru fiecare prelucrare și catalogare;
5. Consimtamantul;
6. Date referitoare la minori;
7. Evaluarea riscurilor de securitate/politica de răspuns la incidente de securitate;
8. Data Protection by design / data protection by default;
9. Drepturile persoanei vizate;
10. DPO - Ofiter protectie date;
11. Transferul de date cu caracter personal către state terțe.

Responsabilul cu protecția datelor - art.37

Principiul responsabilității - art.5 alin.(2) RGPD

Consolidarea rolului operatorului și sporirea responsabilității acestuia

- 1) Definirea și aplicarea măsurilor adecvate și eficace în vederea garantării respectării principiilor;
- 2) Să dovedească îndeplinirea acestor măsuri și să verifice eficacitatea acestora.

DPO - Ofiter protectie date

- 1) Intermediar între diferiți actori (Autoritatea Națională de Supraveghere, persoane vizate, entități din cadrul organizației);
- 2) Desemnare DPO = standard de bune practici - diligență;
- 3) “Piatra de temelie” în scopul respectării principiului responsabilității;
- 4) Facilitează conformitatea cu RGPD.

Operatorul este responsabil de respectarea principiilor legate de prelucrarea datelor cu caracter personal și poate demonstra această respectare („responsabilitate”)

Responsabilul cu protecția datelor - art.37

Desemnare DPO obligatorie

Operator - persoana împuternicită de către operator;
Autoritate sau un organism public, cu excepția instanțelor care acționează în exercițiul funcției lor jurisdicționale;
Activitățile principale constau în operațiuni de prelucrare care, prin natura, domeniul de aplicare și/sau scopurile lor, necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă;
Activitățile principale constau în prelucrarea pe scară largă a unor categorii speciale de date sau a unor date cu caracter personal privind condamnări penale și infracțiuni;
Nu este responsabil în caz de neconformitate a prelucrărilor cu RGPD;
Operatorul sau persoana împuternicită de operator sunt responsabili pentru conformitatea prelucrărilor cu RGPD (art.24 alin.1);
Trebuie să beneficieze de suficientă autonomie și de resursele necesare.

Responsabil cu protecția datelor - art.37 DPO desemnare

Analiza internă - poate fi cerut / impus de Autoritatea Națională de Supraveghere / are natură juridică distinctă - rezultă din statutul acestuia în cadrul organizației, poziție sau funcții / entitatea poate să desemneze o persoană care să gestioneze materia, fără a fi însă DPO dacă nu îndeplinește condițiile expuse ale RGPD;

Un grup de organizatii/societati poate numi un responsabil cu protecția datelor unic, cu condiția ca responsabilul cu protecția datelor să fie ușor accesibil din fiecare organizatie / societate;

- art.37 alin.(4) - desemnarea voluntară sau în temeiul dreptului Uniunii sau dreptului intern (pot să prevadă desemnarea DPO și în alte cazuri decât cele prevăzute expres de RGPD).

Desemnare.

Membru al personalului;

In baza unui contract de prestari servicii.

Activități principale

Activități care privesc funcțiile de bază ale operatorului / persoana împuñnicita. / Privește inclusiv persoana împuñnicită de operator.

Condiții

Calități profesionale / cunoștințe de specialitate în dreptul și practicile din domeniul protecției datelor / capacitatea de a îndeplini sarcinile prevăzute de RGPD.

Protectia datelor: termeni si definitii

Date cu caracter personal	Date cu caracter special
Orice informatii privind o persoana fizica identificata sau identificabila (persoana vizata) , direct sau indirect, cum ar fi nume, prenume, numar de identificare, date de geolocalizare, identificator online (adresa IP, cookie IP) si orice elemente specifice identitatii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale	date privind originea etnica sau rasiala date privind opiniile politice date privind confesiunea religioasa sau convingerile filozofice apartenenta la sindicate date genetice, data biometrice date privind sanatatea date privind viata sexuala sau orientarea sexuala

Prelucrare

Operatiune / set de operatiuni / colectarea / inregistrarea / organizarea / structurarea / stocarea / adaptarea sau modificarea / extragerea / consultarea / utilizarea / divulgarea prin transmitere / diseminarea sau punerea la dispozitie prin orice alt mod / alinierea sau combinarea / restrictionarea / stergerea sau distrugerea.

Protectia datelor: termeni si definitii

Operator	Persoana imputernicita de operator	Reprezentant
Persoana fizica sau juridica, autoritatea publica, agentia sau alt organism care, singur sau impreuna cu altele, stabeleste scopurile si mijloacele de prelucrare a datelor cu caracter personal	Persoana fizica sau juridica, autoritatea publica, agentia sau alt organism care prelucreaza datele cu caracter personal in numele operatorului	Persoana fizica sau juridica stabilita in Uniune, desemnata in scris de un operator sau de o persoana imputernicita de operator, ambele cu sediul in afara UE, care reprezinta operatorul sau persoana imputernicita de operator in ceea ce priveste obligatiile ce le revin in temeiul Regulamentului General pentru Protectia Datelor

Aplicabilitate materiala

Toate prelucrările de date cu caracter personal.

Prelucrări efectuate de o persoană fizică în cadrul unei activități exclusiv personale sau domestice;

Prelucrări realizate de autoritățile competente în scopul prevenirii și combaterii infracțiunilor – Directiva 2016/680 ;

Activități care nu intră sub incidența dreptului UE

Activități care intră sub incidența cap. 2 titlul V din Tratatul UE

Aplicabilitate teritorială

RGPD este aplicabil:

1) Prelucrarilor de date personal în cadrul activităților unui sediu al unui operator sau al unui imputernicit pe teritoriul Uniunii:

Chiar dacă prelucrarea nu are loc pe teritoriul Uniunii;

Sediul presupune exercitarea unei activități în mod efectiv și real indiferent de dimensiune.

2) Prelucrările de date personale ale unor persoane vizate aflate în Uniune, efectuate de un operator sau împoternicit care nu e stabilit în Uniune, dacă prelucrările sunt legate de:

Oferirea de bunuri sau servicii către persoane aflate în Uniune;

Monitorizarea comportamentului persoanelor din Uniune .

3) Regulamentul se poate aplica unor imputerniciti din afara Uniunii atunci cand:

- Incheie un contract cu un operator sau imputernicit care este stabilit în Uniune.

- Incheie un contract cu un operator sau un imputernicit care nu este stabilit în Uniune, dar ofera bunuri și servicii/monitorizează comportamentul unor persoane din Uniune.

4) În caz de extraterritorialitate, ca regula, operatorul sau imputernicitorul are obligația numirii unui reprezentant în statul membru în care se află persoanele vizate.

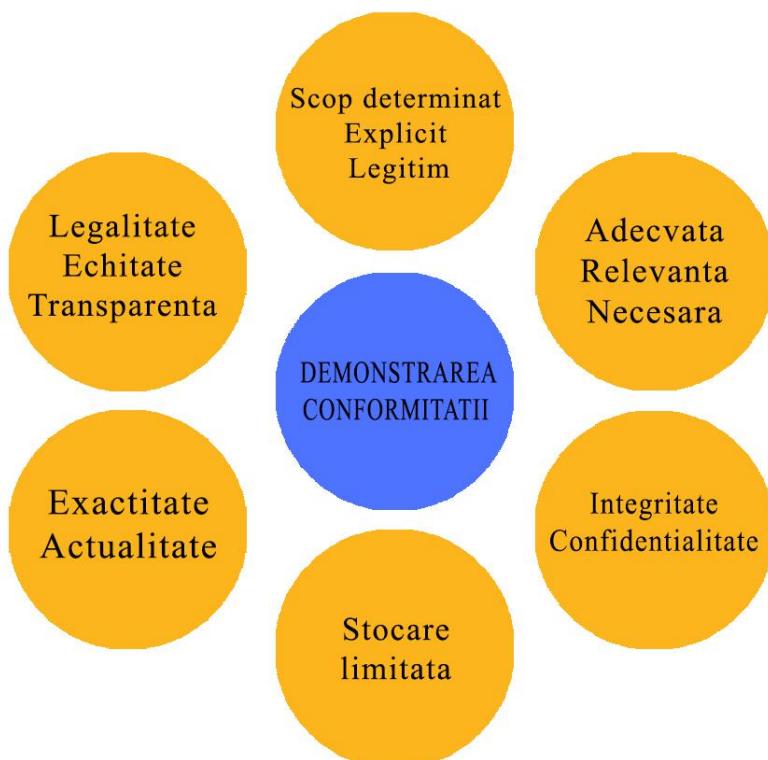
Principiile si temeiurile prelucrarii

Orice prelucrare trebuie realizata:

- 1) Cu respectarea principiilor prelucrarii datelor,
- 2) In baza unuia dintre temeiurile expres prevazute de Regulament General pentru Protectia Datelor,
- 3) Avand capacitatea de a demonstra respectarea prevederilor Regulamentului General pentru Protectia Datelor.

Prelucrarea datelor fara respectarea principiilor sau fara existenta unui temei pentru prelucrare poate fi sanctionata cu amenda pana la 4% din cifra de afaceri globala anuala sau pana 20.000.000 EUR, luandu-se in calcul cea mai mare valoare.

Principiile prelucrarii datelor

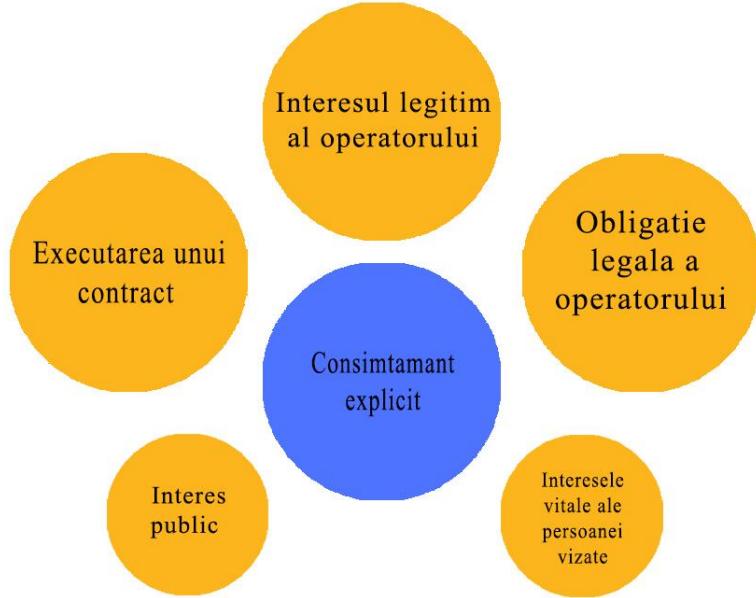


Principiile prelucrarii datelor

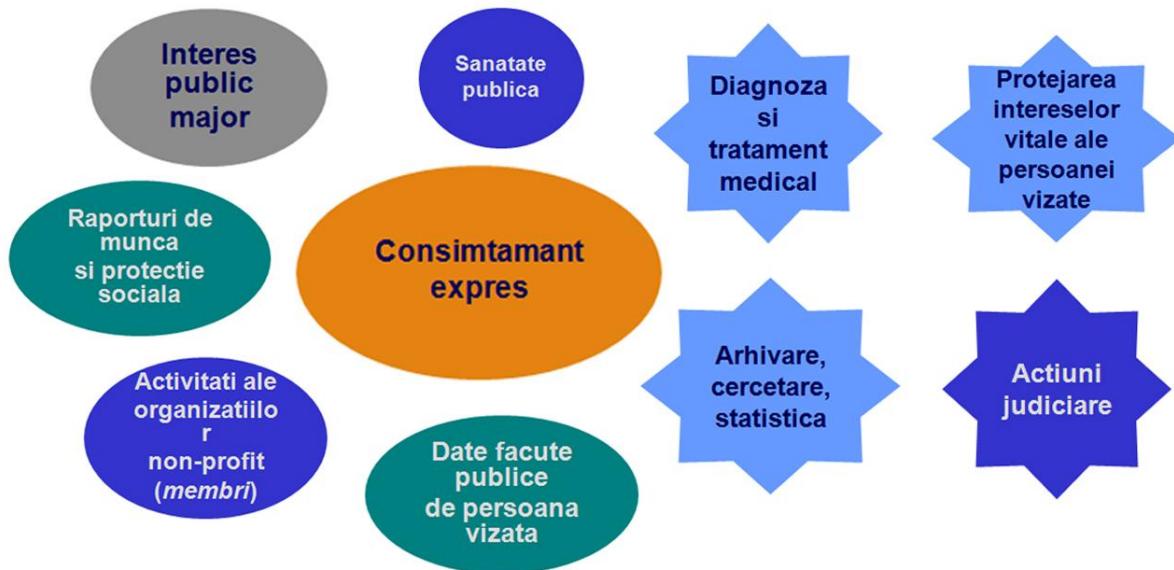
Modificari aduse de Regulamentul General pentru Protectia Datelor:

- 1) principiile sunt actualizate, mai bine definite;
- 2) principiul prelucrarii neexcesive este inlocuit cu principiul prelucrarii limitate la ceea ce este necesar (principiul minimizarii datelor);
- 3) principiul stocarii limitate trebuie vazut prin comparatie cu noul drept al persoanei vizate – dreptul de a fi uitat;
- 4) principiul prelucrarii transparente trebuie avut in vedere de operatori la definirea si implementarea operatiunilor de prelucrare;
- 5) principiul responsabilitatii (accountability) este introdus; operatorul nu trebuie numai sa asigure respectarea principiilor, trebuie sa fie capabil sa dovedeasca faptul ca le respecta.

Temeiurile prelucrarii datelor



Temeiurile prelucrarii datelor cu caracter special



Conditii – consimtamant valabil

1) Consimtamant:

Orice indicatie liber exprimata, specifica, in cunostinta de cauza si clara acordata printr-o declaratie sau o actiune fara echivoc;

2) Liber exprimat:

Consimtamantul nu este valabil daca persoana vizata nu are o alegere reala sau este in imposibilitatea de a refuza sau de a-si retrage consimtamantul cand exista un dezechilibru intre operator si persoana vizata.

3) In cunostinta de cauza (informat).

Operatorul se asigura ca:

Foloseste o maniera inteligibila si usor accesibila, utilizand un limbaj clar si simplu;

Informeaza persoana vizata cel putin cu privire la identitatea operatorului, datele de contact ale responsabilului cu protectia datelor, dupa caz, scopul(urile) prelucrarii, destinatarii datelor, statele catre care

sunt transferate datele, dupa caz.

4) Cererea de consimtamant distincta de orice alte aspecte:

In cazul unei declaratii care se refera si la alte aspecte, cererea privind obinerea consimtamantului trebuie sa fie prezentata distinct, intr-o maniera inteligibila, accesibila, utilizant un limbaj clar si simplu;

5) Dovada consimtamantului:

Regulamentul prevede in mod expres ca operatorul trebuie sa fie capabil sa dovedeasca obtinerea consimtamantului;

6) Dreptul persoanei vizate de a-si retrage consimtamantul:

Regulamentul recunoaste in mod expres acest drept;

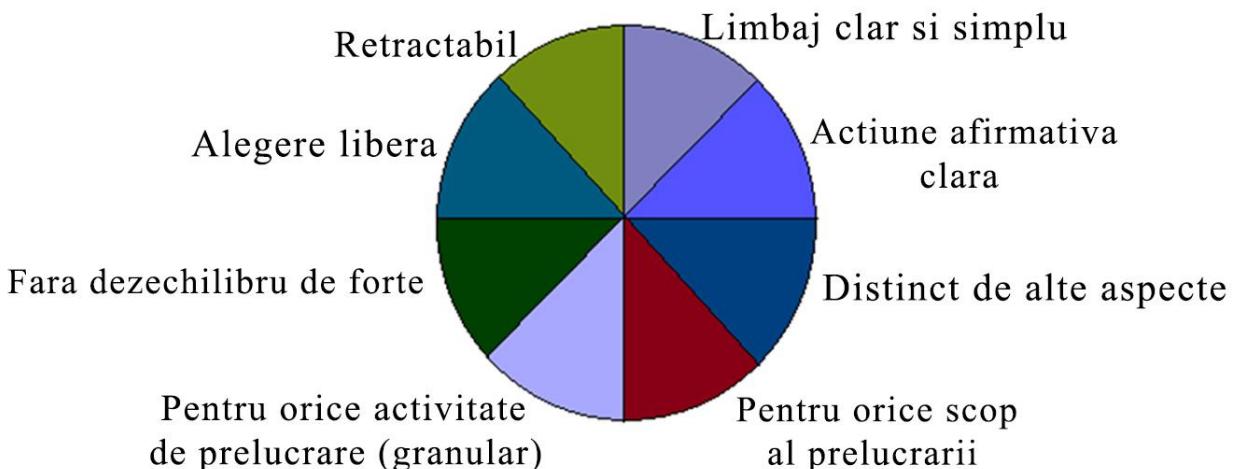
Persoana vizata trebuie informata cu privire la dreptul de retragere anterior obtinerii consimtamantului;

Dreptul de retragere trebuie sa poata fi exercitat usor (in aceeasi maniera in care a fost acordat);

Dupa retragerea consimtamantului, prelucrarea poate continua numai daca exista un alt temei pentru prelucrare.

Conditii – consimtamant valabil

Consimtamantul acordat anterior datei de 25 mai 2018 poate ramane temei legal pentru prelucrarea datelor cu caracter personal ulterior datei de aplicare a Regulamentului General pentru Protectia Datelor daca intruneste conditiile de validitate prevazute de Regulament:



Drepturile persoanelor vizate

Lista drepturi (anterior)	Lista drepturi (dupa 25 mai 2018)
Informare (art. 12)	Informare (art. 13, art. 14)
Acces (art. 13)	Acces (art. 15)
Interventie (art. 14)	Rectificare (art. 16, art. 19)
	Stergere (art. 17, art. 19)
	Restrictionare (art. 18, art. 19)
	Portabilitate (art. 20)
Opozitie (art. 15)	Opozitie (art. 21)
Decizii automate individuale (art. 17)	Decizii automate, profilare (art. 22)
Restrictii (art. 16)	Restrictii (art. 23)

Dreptul de informare – sursa directă

Identitatea si datele de contact ale operatorului;
Datele de contact ale DPO;
Scopurile, temeiul juridic, interesul legitim urmarit, destinatarii, detalii privind un eventual transfer;
Perioada de stocare (criteriile utilizate);
Existenta drepturilor de acces, rectificare, stergere, opozitie, restrictionarea prelucrarii, portabilitatea datelor, a dreptului de retragere a consimtamantului, de a depune o plangere;
Daca furnizarea datelor decurge dintr-o obligatie legala sau contractuala si care sunt consecintele refuzului;
Existenta unui proces decizional, crearea de profiluri, logica utilizata, importanta si efectele unei astfel de prelucrari.

Dreptul de informare – sursa indirecta

Identitatea si datele de contact ale operatorului

Datele de contact ale DPO

Scopurile, temeiul juridic.

Categorii de date.

Destinatarii, detalii privind un eventual transfer;

Perioada de stocare (criteriile utilizate);

Existenta drepturilor de acces, rectificare, stergere, opozitie.

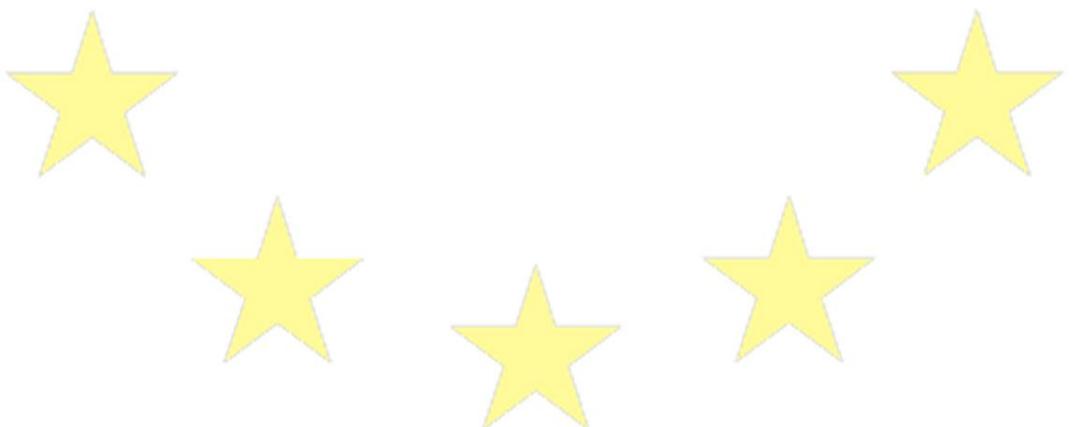
Restrictionarea prelucrarii, portabilitatea datelor, a dreptului de retragere a consumatorului, de a depune o plangere

Sursa datelor

Daca furnizarea datelor decurge dintr-o obligatie legala sau contractuala si care sunt consecintele refuzului

Existenta unui proces decizional, crearea de profiluri, logica utilizata, importanta si efectele unei astfel de prelucrari

Scopul prelucrarii ulterioare



Dreptul de informare – exceptii

Sursa directa

Persoana detine deja informatiile.

Sursa indirecta

Persoana detine deja informatiile;

Furnizarea se dovedeste imposibila sau implica eforturi disproportionate (in special arhivare, cercetare sau statistica);

In masura in care obligatia este susceptibila sa faca imposibila sau sa afecteze in mod grav realizarea obiectivelor prelucrarii respective, cu conditia de a lua masuri adecvate pentru a proteja drepturile, libertatile si interesele legitime ale persoanei vizate, inclusiv punerea informatiilor la dispozitia publicului;

Obtinerea sau divulgarea este prevazuta de dreptul UE/intern;

Respectarea confidențialității conform unei obligații statutare/legale de păstrare a secretului.

Pictograma informare



Dreptul de acces

Confirmare ca sunt sau nu prelucrate datele

Acces la date si la urmatoarele informatii:

Scopurile prelucrarii;

Categoriile de date;

Destinatarii, inclusiv din state/organizatii internationale terte;

Perioada de stocare (criteriile utilizate);

Existenta drepturilor de acces, rectificare, stergere, opozitie, restrictionare, portabilitate, a dreptului de retragere a consimtamantului, de a depune plangere;

Sursa de colectare a datelor;

Existenta unui proces decizional, crearea de profiluri, logica utilizata, importanta si efectele unei astfel de prelucrari;

Garantiile ce insotesc un eventual transfer;

Copie a datelor prelucrate;

Copii ulterioare - taxa rezonabila (costuri administrative).

LIMITE:

Furnizarea copiei sa nu aduca atingere drepturilor si libertatilor altor persoane.

Dreptul la rectificare

Rectificarea datelor cu caracter personal inexakte care o privesc, fara intarzieri nejustificate.

Completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declaratii suplimentare.

Dreptul la stergere (“dreptul de a fi uitat”)

Stergerea datelor, fara intarzieri nejustificate se va face daca:

- 1) Datele nu mai sunt necesare pentru indeplinirea scopurilor;
- 2) Persoana vizata isi retrage consimtamantul;
- 3) Persoana se opune prelucrarii si nu exista motive de prevalenta a intereselor operatorului;
- 4) Datele au fost prelucrate ilegal;
- 5) Datele trebuie sterse conform obligatiilor dreptului Uniunii/intern;
- 6) Datele au fost furnizate in legatura cu oferirea de servicii ale societatii informationale.

Informarea operatorilor care prelucreaza datele in legatura cu cererea persoanei vizate de stergere a unor linkuri, copii sau reproduceri, daca datele au fost publicate (masuri rezonabile, inclusiv tehnice).

Dreptul la stergere (“dreptul de a fi uitat”)

EXCEPTII

Prelucrarea este necesara pentru:

- 1) Exercitarea dreptului la libera exprimare si la informare;
- 2) Respectarea unei obligatii legale conform dreptului Uniunii/intern ori a unei sarcini publice/autoritati oficiale;
- 3) Motive de interes public in domeniul sanatatii publice;

- 4) Scopuri de arhivare in interes public, in scopuri de cercetare stiintifica sau istorica ori in scopuri statistice, in masura in care dreptul la stergere este susceptibil sa faca imposibila sau sa afecteze in mod grav realizarea obiectivelor prelucrarii respective;
- 5) Constatarea, exercitarea sau apararea unui drept in instanta.

Dreptul la restrictionare

Marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora.

SITUATII:

- 1) se contesta exactitatea datelor, pentru o perioada care ii permite operatorului sa verifice exactitatea datelor
- 2) prelucrarea este ilegală, iar persoana vizata se opune stergerii datelor cu caracter personal, solicitand in schimb restrictionarea utilizarii lor
- 3) operatorul nu mai are nevoie de datele cu caracter personal in scopul prelucrarii, dar persoana vizata i le solicita pentru constatarea, exercitarea sau apararea unui drept in instanta
- 4) persoana vizata s-a opus prelucrarii, pentru intervalul de timp in care se verifica daca drepturile legitime ale operatorului prevaleaza asupra celor ale persoanei vizate

Dreptul la restrictionare

LIMITE:

Prelucrare posibila pe perioada restrictionarii:

- 1) Cu consimtamantul persoanei vizate;
- 2) Pentru constatarea, exercitarea sau apararea unui drept in instanta;
- 3) Pentru protectia drepturilor unei alte persoane fizice sau juridice; 4) Din motive de interes public important al Uniunii sau al unui stat membru;

Dreptul la portabilitate

Primirea datelor si transmiterea catre alt operator, intr-un format structurat, utilizat in mod curent si care poate fi citit automat, interoperabil

Conditii de exercitare:

- 1) Datele privesc solicitantul (persoana vizata);
- 2) Datele au fost furnizate de persoana vizata;
- 3) Prelucrarea se bazeaza pe consintamant/contract;
- 4) Prelucrarea se efectueaza prin mijloace automate.

LIMITE:

- 1) Prelucrarea necesara pentru indeplinirea unei sarcini executate in interes public sau in cadrul exercitarii unei autoritati oficiale cu care este investit operatorul;
- 2) Nu aduce atingere drepturilor si libertatilor altora.

Dreptul la opozitie

Opozitia fata de prelucrarea datelor si crearea de profiluri, din motive legate de situatia particulara in care se afla persoana vizata / marketing direct.

Conditii suplimentare:

Informare cu privire la existenta acestui drept in mod explicit, prezentat in mod clar si separat de orice alte informatii, cel tarziu in momentul primei comunicari cu persoana vizata.

LIMITE:

- 1) motive legitime si imperioase care justifica prelucrarea si care prevaleaza asupra intereselor, drepturilor si libertatilor persoanei vizate;
- 2) scopul este constatarea, exercitarea sau apararea unui drept in instantă;
- 3) in scopuri de cercetare stiintifica sau istorica sau in scopuri statistice, prelucrarea este necesara pentru indeplinirea unei sarcini din motive de interes public.

Proces decizional individual automatizat, inclusiv crearea de profiluri

- 1) Dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automata, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizata sau o afecteaza in mod similar intr-o masura semnificativa;
- 2) Decizia nu trebuie sa aiba la baza date sensibile.

LIMITE:

- 1) Decizia este necesara pentru incheierea sau executarea unui contract intre persoana vizata si un operator de date;
- 2) Decizia are la baza consimtamantul explicit al persoanei vizate;
- 2.1) Operatorul de date pune in aplicare masuri corespunzatoare pentru protejarea drepturilor, libertatilor si intereselor legitime ale persoanei vizate, cel putin dreptul acesteia de a obtine interventie umana din partea operatorului, de a-si exprima punctul de vedere si de a contesta decizia;

3) Decizia este autorizata prin dreptul Uniunii sau dreptul intern care se aplica operatorului si care prevede, de asemenea, masuri corespunzatoare pentru protejarea drepturilor, libertatilor si intereselor legitime ale persoanei vizate.

Exercitarea drepturilor

Transparentă

Condiții

- 1) limbaj clar, simplu (minor);
- 2) formă concisă, transparentă, inteligibilă și ușor accesibilă;
- 3) în scris/electronic/verbal;
- 4) gratuit (excepții – refuz, taxa rezonabilă).

Termene

Intre 1 si 3 luni;

1 luna – prelungire termen/refuz adoptare masuri + motive + drept plangere ANSPDCP + actiune in instanta.

Drepturi noi pentru persoana vizata

Unul din obiectivele Regulamentului General pentru Protectia Datelor este acela de a oferi persoanelor vizate un control asupra propriilor date cu caracter personal:

- 1) pastreaza drepturile existente;
- 2) consolideaza drepturile existente;
- 3) reglementeaza drepturi noi: dreptul de a fi uitat, dreptul la restrictionarea prelucrarii, dreptul la portabilitatea datelor;

Nerespectarea drepturilor persoanei vizate poate fi sancționată cu amenda până la 4% din cifra de afaceri globala anuala sau până la 20.000.000 EUR, luându-se în calcul cea mai mare valoare.

Recomandari de bune practici

Transparență (site) / Proceduri privind exercitarea drepturilor / Formulare specifice / Instruirea personalului / Consultarea DPO/ANSPDCP.



Obligatii ale operatorilor care prelucreaza date cu caracter personal.

Regulamentul General pentru Protectia Datelor creeaza un cadrul din care rezulta o serie de obligatii pentru operatorii de date, inclusiv:

- 1) Se supun principiului responsabilitatii (accountability) potrivit caruia trebuie sa se conformeze si sa demonstreze conformitatea;
- 2) Asigura respectarea principiilor protectiei datelor cu caracter personal atat la momentul conceperii activitatilor de prelucrare (privacy by design), cat si in mod implicit (privacy by default);
- 3) Au obligatia de a notifica incalcarea securitatii datelor;
- 4) Incalcarea unei obligatii poate fi sancionata cu amendă pana la 2% sau pana la 4% din cifra de afaceri globala anuala sau pana la 10.000.000 EUR sau 20.000.000 EUR, luandu-se in calcul cea mai mare valoare.



SECURITATEA PRELUCRARII

Prin masuri tehnice si organizatorii, incluzand printre altele:

- 1) Pseudonimizarea si criptarea datelor cu caracter personal;
- 2) Capacitatea de a restabili disponibilitatea datelor cu caracter personal si accesul la acestea in caz de incident; 3) Testare si evaluare periodice ale masurilor implementate;
- 4) Capacitatea de a asigura confidentialitatea, integritatea, disponibilitatea si rezistenta sistemelor de prelucrare;

Aderarea la un cod de conduită sau la un mecanism de certificare aprobat poate fi o formă de a demonstra indeplinirea obligației de asigurare a securității datelor.

NOTIFICAREA INCALCARII SECURITATII DATELOR

O incalcare a securitatii care duce, in mod accidental sau ilegal, la distrugerea, pierderea, modificarea sau divulgarea neautorizata a datelor cu caracter personal transmise, stocate sau prelucrate intr-un alt mod sau la accesul neautorizat la acestea.

- 1) Operatorul tine evidența tuturor incalcarilor;
- 2) Dacă incalcarea generează un risc pentru persoana vizată:
 - 2.1) Incalcarea este notificată ANSPDCP fără întârzieri nejustificate, în termen de cel mult 72 de ore;
 - 2.2) Notificarea include descrierea incalcerii, posibile consecințe și măsuri de remediere sau diminuare a efectelor, precum și contactarea DPO;

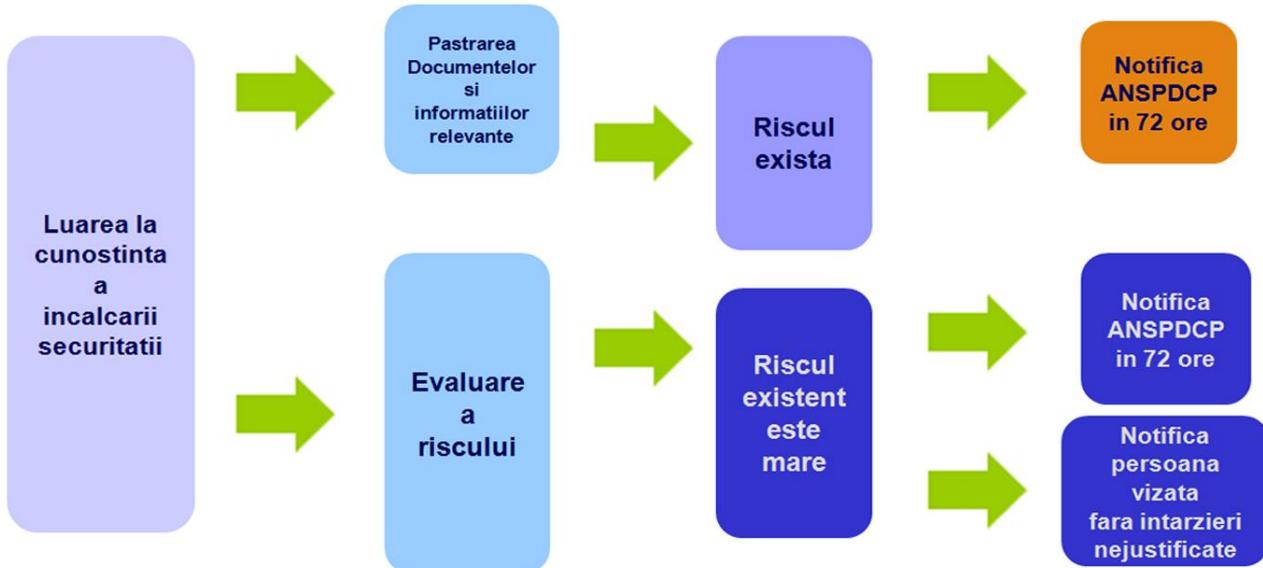
NOTIFICAREA INCALCARII SECURITATII DATELOR

- 1) In situatia in care incalcarea genereaza un risc ridicat pentru drepturile si libertatile persoanelor fizice incalcarea este notificata fara intarzieri nejustificate persoanei vizate;
- 2) Risc pentru drepturile si libertatile persoanelor fizice - prejudicii fizice, materiale sau morale:

Pierdere sau limitarea controlului / Pierdere financiara / Discriminare / Compromiterea reputatiei / Furt de identitate / Dezavantaj economic sau social.

EXCEPTIE

Operatorul poate fi exonerat de notificarea catre persoana vizata daca datele sunt protejate (prin criptare), au fost luate masuri de protectie sau notificarea cere eforturi disproportionate.

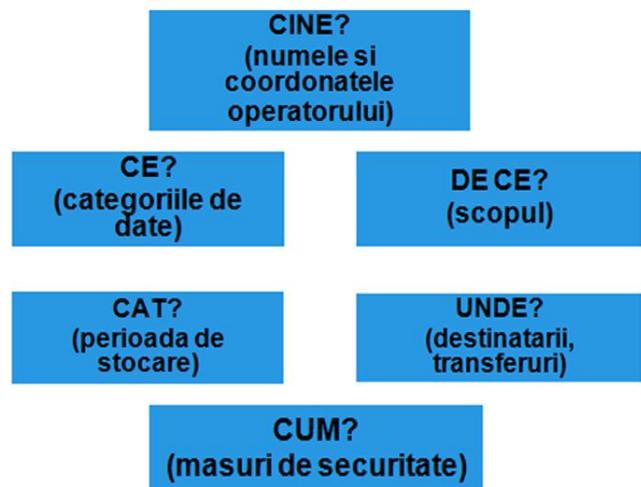


CARTOGRAFIEREA

Art. 30 din RGPD se aplică:

- Operatorilor din sistemul public
- Persoanelor împoternicite de operator
- Operatorilor din sectorul privat cu peste 250 de angajați

Desființarea actualului sistem de notificare a prelucrărilor de date la ANSPDCP



Obligatia de a numi un responsabil cu protectia datelor, daca sunt indeplinite conditiile prevazute de Regulamentul General pentru Protectia Datelor;

Raspundere solidara in situatia operatorilor asociati;

Raspund la solicitarile de exercitare a drepturilor reglementate de Regulamentul General pentru Protectia Datelor.

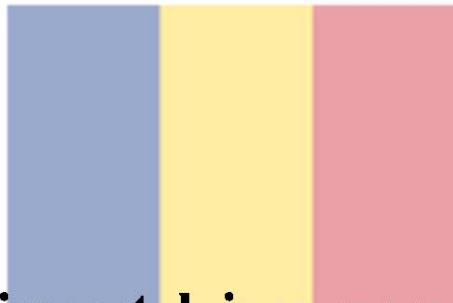
Obligatiile persoanelor imputernicite

- 1) Obligatia de pastra evidenta activitatilor de prelucrare desfasurate in numele operatorului;
- 2) Obligatia de a notifica operatorului fara intarzieri nejustificative orice incalcare a securitatii datelor cu caracter personal;
- 3) Obligatia de a numi un responsabil cu protectia datelor, daca sunt indeplinite conditiile prevazute de Regulamentul General pentru Protectia Datelor;
- 4) Obligatia de a respecta regulile privind transferul de date in afara tarii/Uniunii
- 5) Raspundere directa fata de persoana vizata daca a incalcat o obligatie

prevazuta de Regulamentul General pentru Protectia Datelor direct in sarcina sa sau a actionat in afara instructiunilor operatorului;

6) In situatia in care o persoana imputernicita incalca prevederile Regulamentului General pentru Protectia Datelor, prin luarea de decizii cu privire la scopul si mijloacele prelucrarii datelor cu caracter personal, devine ea insasi operator cu toate obligatiile asociate.

Obligatiile persoanelor imputernicite



Evaluarea impactului: ce reprezinta, cand este necesara

- 1) O analiza pas cu pas a activitatilor de prelucrare care sa ajute operatorul sa identifice si sa analizeze toate riscurile pe care acestea le pot genera;
- 2) Realizata de operator cu sprijinul responsabilului cu protectia datelor;
- 3) Se impune in cazul prelucrarilor susceptibile sa genereze un **risc** ridicat precum:
 - 3.1) evaluarea sistematica si cuprinsatoare prin mijloace automate care stau la baza unei decizii care produce efecte juridice asupra persoanei fizice (ex. profiling, predicting)
 - 3.2) prelucrarea pe scara larga a unor categorii speciale de date cu

caracter personal (ex. date biometrice, date genetice) sau date privind condamnarile penale si infractiuni

3.3) monitorizarea sistematica pe scara larga a unei zone accesibile publicului (ex. CCTV).

4) O lista a tipurilor de operatiuni pentru care este necesara evaluarea intocmita si publicata de autoritatea de supraveghere;

5) Criterii pentru stabilirea prelucrarilor cu risc ridicat:

5.1) Prelucrarea este de tip evaluare, scoring, profiling, predicting;

5.2) Produce efecte juridice asupra persoanei fizice;

5.3) Presupune monitorizare sistematica;

5.4) Presupune date personale cu caracter special;

5.5) Presupune prelucrare la scara larga (numar de persoane vizate, volum de date, durata prelucrarii, intinderea geografica a prelucrarii);

5.6) Presupune combinarea unor date provenite din prelucrari diferite;

5.7) Priveste persoane vulnerabile (angajati, minori);

5.8) Presupune tehnologii noi.

Responsabilul cu protectia datelor

ESTE OBLIGATORIU PENTRU:

- **autoritățile publice**, cu excepția instanțelor judecătorești
- operatorii care realizează o **monitorizare pe scară largă** a persoanelor fizice
- operatorii care prelucrează pe scară largă unele **categorii speciale de date** prevăzute de art. 9 și 10
(ex. origine etnică, orientare politică, religioasă, date genetice, biometrice, privind sănătate sau referitoare la infracțiuni)

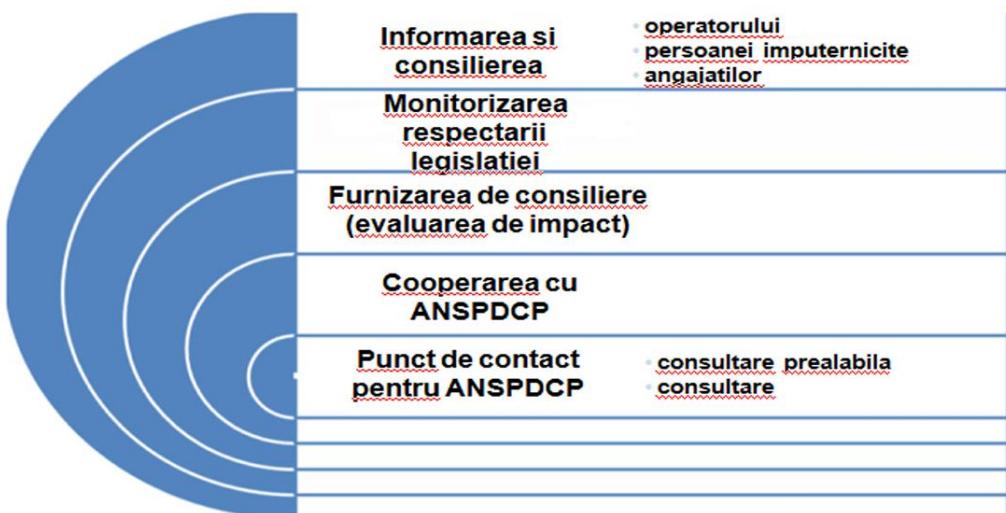


Responsabilul cu protectia datelor cu caracter personal (DPO) poate fi numit din cadrul operatorului / imputernicitului si este in subordinea conducerii organizatiei / societatii , avand statut special. DPO poate fi angajat pe baza de contract de prestari servicii.

Condiții de numire DPO art. 37 RGPD

- 1) Calități profesionale;
- 2) Cunoștințe de specialitate în dreptul și practicile din domeniul protecției datelor;
- 3) Capacitatea de îndeplinire a sarcinilor;
- 4) Independență - nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea sarcinilor;
- 5) Răspunde direct în fața celui mai înalt nivel al conducerii operatorului / persoanei imputernicite;
- 6) Protecție specială - nu poate fi demis sau sancționat de către operator / imputernicit pentru îndeplinirea sarcinilor sale;
- 7) Obligația de a respecta confidențialitatea în îndeplinirea sarcinilor sale.

Obligatii si responsabilitati



Operatorul/persoana împuternicită de operator are obligația:

- 1) De a publica datele de contact ale responsabilului cu protecția datelor (adresa operatorului, număr de telefon și/sau o adresă de e-mail profesională a responsabilului);
- 2) De a comunica ANSPDCP datele de contact ale responsabilului cu protecția datelor.

Transferul de date în state terțe

Regulile privind transferul de date în afara Uniunii

Transferurile de date sunt posibile doar:

- 1) Catre un stat căruia Comisia Europeană i-a recunoscut un nivel de protecție adecvat (Andora, Argentina, Canada, Elveția, Insulele Feroe, Guernsey, Israel, Insula Man, Jersey, Uruguay și Noua Zeelandă) sau
- 2) Dacă transferul are loc în baza unor garantii adecvate;

Transferul în baza oricărui dintre temeiurile de mai sus nu necesită vreo aprobare/autorizare din partea Comisiei Europene sau a autoritatii de supraveghere;

Regulamentul General pentru Protectia Datelor prevede că sunt supuse acelorași reguli și transferurile ulterioare (onward transfers).

Cooperare internațională

Măsuri corespunzătoare ale CE și autorităților de supraveghere

- 1) Elaborarea de mecanisme de cooperare internațională;
- 2) Acordarea de asistență internațională reciprocă;
- 3) Implicarea părților interesate relevante, în scopul intensificării cooperării internaționale;
- 4) Promovarea schimbului reciproc și a documentației (legislație, practici, conflicte jurisdicționale).

Autoritatea de supraveghere principală

Autoritatile de supraveghere vor avea în continuare competența de a reglementa și aplica prevederile în domeniul protecției datelor cu caracter personal care afectează statul membru;

În cazul organizațiilor care își desfășoară activitățile în mai multe state membre, autoritatea de supraveghere de la sediul principal va fi autoritate de supraveghere principală;

Autoritatea de supraveghere din statul membru în care se află persoana vizată acționează ca punct de contact atunci când operatorul este stabilit într-un alt stat.

Sanctiuni

2% din cifra de afaceri mondială totală anuală sau 10.000.000 EUR, luându-se în calcul cea mai mare valoare	4% din cifra de afaceri mondială totală anuală sau 20.000.000 EUR, luându-se în calcul cea mai mare valoare
Incalcarea obligațiilor de către operator/persoana imputernicita	Incalcarea principiilor pentru prelucrare, inclusiv condițiile privind consumatorul
Incalcarea obligațiilor de către organismul de certificare	Incalcarea drepturilor persoanelor vizate
Incalcarea obligațiilor de către organismul de monitorizare a unui cod de conduită	Incalcarea regulilor privind transferul de date cu caracter personal către state terțe sau organizații internaționale
	Incalcarea legislației emise în temeiul marjei naționale de reglementare
	Incalcarea unui ordin sau a unei limitări temporare sau definitive asupra prelucrării sau a suspendării fluxurilor de date emisă de autoritatea de supraveghere