Regulamentul General privind Protecția Datelor (GDPR) (UE) 2016/679 pe scurt

Ce este GDPR ?

GDPR este un Regulament european cu scopul:

- ✓ protejării prelucrărilor de date cu caracter personal;
- ✓ reglementării liberei circulații a datelor cu caracter personal;
- ✓ protejării drepturilor si libertăților persoanelor fizice cu privire la datele lor cu caracter personal;

Conform: art. (1), par. (1) – (13)

Cui se aplica GDPR ?

Operatorului și persoanei împuternicite din cadrul UE, indiferent unde are loc prelucrarea de date;
Operatorului și persoanei împuternicite din afara UE, în cazul in care:

- ✓ oferă bunuri si servicii către persoane de pe teritoriul UE;
- ✓ monitorizează comportamentul persoanelor fizice din UE;

Conform: art. (3), par. (22) – (25)

Principii generale

Principiile prelucrării datelor
Prelucrarea datelor trebuie sa fie:
- ✓ legală
- ✓ echitabilă
- ✓ transparentă

Principiile colectarii datelor
Colectarea datelor trebuie să fie:
- ✓ pentru utilizări specifice
- ✓ explicită
- ✓ scopuri legitime

Reducerea la minimum a datelor pe care le cerem/prelucrăm
Datele trebuie să fie:
- ✓ adecvate
- ✓ relevante
- ✓ limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate

Acuratețea

Datele cu caracter personal trebuie sa fie:
- ✓ exacte
- ✓ unde e cazul, actualizate

Trebuie luate masuri rezonabile ca datele care nu sunt exacte să fie:
- ✓ șterse
- ✓ rectificate fără întârziere

Limitări legate de stocare

Regulă: datele cu caracter personal nu trebuie păstrate mai mult decât este necesar pentru îndeplinirea scopurilor.

Excepția: datele cu caracter personal pot fi stocate pe perioade mai lungi in măsura în care acestea vor fi prelucrate exclusiv in următoarele scopuri:
- ✓ arhivare in interes public
- ✓ cercetare științifică sau istorică
- ✓ statistic

Integritate si confidențialitate

Datele ar trebui prelucrate într-o manieră care asigură măsuri adecvate de securitate ce includ protecția împotriva:
- ✓ Accesului neautorizat sau prelucrării ilegale;

- ✓ Pierderii sau furtului;
- ✓ Distrugerii
- ✓ Pierderii integrității

Responsabilitate

Operatorul este:
- ✓ responsabil pentru conformitatea cu legislația;
- ✓ în măsura să demonstreze conformitatea cu principiile referitoare la prelucrare.

Conform: art. (5)

Definiții:

Date cu caracter personal = orice informație referitoare la o persoană identificată sau identificabilă („persoana vizată")
Persoana vizată = persoana care poate fi identificată direct sau indirect, prin referire la:
- ✓ un nume
- ✓ un număr de identificare
- ✓ date de localizare
- ✓ un identificator online
- ✓ unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale

Prelucrare de date cu caracter personal = orice operațiune sau set de operațiuni 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 dispoziție in orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.
Restricționarea prelucrării datelor cu caracter personal = marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora.
Crearea de profiluri = orice forma de prelucrare automata a datelor cu caracter personal care consta in utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, in special pentru a analiza sau prevedea aspecte privind performanta la locul de munca, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul in care se afla persoana fizica respectivă sau deplasările acesteia.
Pseudonimizare = prelucrarea datelor cu caracter personal într-un asemenea mod încat acestea sa nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să:
- ✓ fie stocate separat
- ✓ sa facă obiectul unor măsuri de natura tehnică si organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile

Operator = persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreuna cu alte persoane, stabilește scopurile si mijloacele de prelucrare a datelor cu caracter personal
Persoana împuternicită de operator = persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal in numele operatorului

Destinatar = persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) ii sunt divulgate datele cu caracter personal, indiferent daca este sau nu o parte terță
Parte terța = o persoana fizică sau juridică, autoritate publica, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicita de operator si persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate sa prelucreze date cu caracter personal
Consimțământ = orice manifestare de voință liberă, specifică, informată si lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc sa fie prelucrate
Încălcarea securității datelor cu caracter personal = o încălcare a securității care duce, in 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
Date genetice = datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice
Date biometrice = date cu caracter personal care rezulta in urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirma identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice
Date privind sănătatea = înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistenta medicală, care dezvăluie informații despre starea de sănătate a acesteia

Conform: art. (4)

Legalitatea prelucrări

Prelucrarea ar trebui să fie legală dacă se aplică cel puțin una din următoarele:
- ✓ Persoana vizată și-a dat consimțământul
- ✓ Prelucrarea este necesară pentru încheierea sau executarea unui contract
- ✓ Prelucrarea este necesară pentru îndeplinirea unei obligații legal
- ✓ Prelucrarea este necesară pentru a proteja interesele vitale
- ✓ Interesul public
- ✓ Al unui operator sau al unei părți terțe

Conform: art. (6)

Consimtământul

Definiție: orice manifestare de voința a unei persoane având următoarele atribute
- ✓ liberă
- ✓ specifică
- ✓ informată
- ✓ lipsită de ambiguitate

făcută printr-o declarație sau o acțiune fără echivoc cu privire la prelucrarea datelor sale cu caracter personal.

Condiții cu privire la consimțământ:

- ✓ operatorul trebuie să poată face dovada că a obținut consimțământul persoanei
- ✓ diferențiat clar de alte documente
- ✓ forma inteligibilă (să se vadă că a fost clar exprimat)
- ✓ ușor de înțeles
- ✓ sa fie într-un limbaj clar si simplu
- ✓ persoana vizata are dreptul de a-și retrage oricând consimțământul
- ✓ retragerea consimțământului nu afectează legalitatea prelucrării anterioare retragerii
- ✓ persoana vizată trebuie informată despre dreptul de a-și retrage consimțământul
- ✓ retragerea trebuie să se facă la fel de simplu ca acordarea lui

Condiții suplimentare cu privire la consimțământul copiilor:

- ✓ copilul trebuie sa aiba peste 16 ani, statele membre putând reduce vârsta la 13 ani
- ✓ părinții își vor da consimțământul pentru copiii sub 16 ani

Conform: art. (7), art. (8)

Categoriile speciale de date

Este interzisa prelucrarea:

- ✓ datelor cu caracter personal care dezvăluie originea rasială sau etnică
- ✓ opiniilor politice
- ✓ confesiunilor religioase
- ✓ convingerilor filozofice
- ✓ apartenențelor la sindicate
- ✓ datelor genetice
- ✓ datelor biometrice
- ✓ datelor privind sănătatea
- ✓ datelor privind viața sexuală sau orientarea sexuală

Excepții:

- ✓ există un consimțământ explicit în acest sens
- ✓ prelucrarea este necesară în scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă și al securității sociale si protecției sociale
- ✓ prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice
- ✓ prelucrarea este efectuată în cadrul activităților lor legitime și cu garanții adecvate de către o fundație, o asociație sau orice alt organism fără scop lucrativ și cu specific politic, filozofic, religios sau sindical
- ✓ prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod expres de către persoana vizată
- ✓ prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanțele acționează in exercițiul funcției lor judiciare

- ✓ prelucrarea este necesară din motive de interes public major
- ✓ prelucrarea este necesara in scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistența socială
- ✓ prelucrarea este necesara din motive de interes public în domeniul sănătății publice, cum ar fi protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau
- ✓ asigurarea de standarde ridicate de calitate și siguranța a asistenței medicale și a medicamentelor sau a dispozitivelor medicale
- ✓ prelucrarea este necesară în scopuri de arhivare în interes public, in scopuri de cercetare științifică sau istorica ori in scopuri statistice
- ✓ prelucrarea datelor cu caracter personal referitoare la condamnări penale si infracțiuni
- ✓ se efectuează numai sub controlul unei autorități de stat sau
- ✓ atunci când prelucrarea este autorizată de dreptul Uniunii sau de dreptul intern.

Conform: art. (9), art. (10)

Transparența

Operatorul trebuie sa ia măsuri adecvate in privința transparenței:

- ✓ cu privire la orice comunicare in temeiul art. (15)-(22) (drepturile persoanei vizate)
- ✓ cu privire la incidentele de securitate (art. 34)
- ✓ cu privire la prelucrarea datelor cu caracter personal
- ✓ să fie într-o forma concisa, transparentă, inteligibilă si accesibilă
- ✓ informația va fi furnizată în scris, incluzând, acolo unde este posibil, formatul electronic

dacă persoana vizată cere, informația poate fi furnizată oral, dar cu dovada aducerii la cunoștință

Exercitarea drepturilor

- ✓ facilitarea exercitării drepturilor persoanei vizate în temeiul art. (15)-(22) (drepturile persoanei vizate)
- ✓ excepție: dacă operatorul este în măsura să demonstreze ca nu poate identifica persoana vizată.

Furnizarea informației despre acțiunile întreprinse

- ✓ operatorul trebuie să furnizeze persoanei vizate informații despre acțiunile întreprinse în temeiul art. (15)-(22) (drepturile persoanei vizate) fără întârziere .

Regula: se face in cel mult 30 de zile de la primirea cererii

Excepție: perioada poate fi extinsă până la 60 de zile, în funcție de complexitatea și numărul cererilor

- ✓ dacă cererea este făcută de către persoana vizată în format electronic, răspunsul trebuie să fie tot in format electronic, cu excepția situației în care persoana vizată solicită altfel (inclusiv oral)
- ✓ dacă operatorul nu acționează, va informa persoana vizată fără întârziere despre motivele refuzului și despre posibilitatea de a depune o plângere la Autoritatea de Supraveghere în cel mult o luna de la primirea cererii.

Gratuitate

- ✓ informația furnizată in temeiul Art. (13) – (14) (informarea persoanei vizate) si comunicările sau măsurile întreprinse in temeiul art. Art. (15)-(22) (drepturile persoanei vizate) trebuie sa fie gratuite

- ✓ când cererea este neîntemeiată sau abuzivă, în special din cauza caracterului repetitiv, operatorul poate:
  - percepe o taxa rezonabilă
  - refuză să dea curs cererii (operatorul trebuie sa fie in măsura să demonstreze că cererea este abuzivă)

Solicitarea de informații suplimentare

Dacă operatorul are un dubiu cu privire la identitatea persoanei, poate solicita acesteia din urma informații suplimentare pentru a-i confirma identitatea.

Conform: art. (11), art. (13)-(14), art. (15)-(22), art. (10), art. (34)

Informațiile care trebuie furnizate persoanei vizate

Când datele sunt colectate direct de la persoana vizată, la momentul la care datele personale sunt colectate, operatorul trebuie să furnizeze persoanei vizate următoarele:

- ✓ identitatea și datele de contact ale operatorului sau ale reprezentantului
- ✓ datele de contact ale responsabilului cu protecția datelor, daca e cazul
- ✓ temeiurile legale și scopurile prelucrării
- ✓ destinatarii sau categoriile de destinatari, daca e cazul.
- ✓ Intenția de a transfera datele către țări din afara SEE sau organizații internaționale
- ✓ perioada de stocare
- ✓ drepturile persoanei vizate
- ✓ dacă datele sunt necesare pentru încheierea sau executarea unui contract, obligația de a furniza datele și consecințele nefurnizării
- ✓ existența unor decizii automate, inclusiv profilarea, logica din spatele acestor procese și consecințele pentru persoana vizată.

Când datele sunt obținute din alta sursă:

- ✓ aceleași informații ca la punctul anterior
- ✓ suplimentar: categoriile de date, sursa

Când trebuie furnizate persoanei vizate?

- ✓ într-un termen rezonabil după obținerea datelor (nu mai mult de o lună);
- ✓ dacă datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana vizată, cel târziu în momentul primei comunicări către persoana vizata respectivă; sau
- ✓ dacă se intenționează divulgarea datelor cu caracter personal către un alt destinatar, cel mai târziu la data la care acestea sunt divulgate pentru prima oara

Conform: expunerea (60)-(62), (65), art. (13)-(14)

Dreptul de acces

- ✓ dreptul de a obține o confirmare ca datele se prelucrează

- ✓ dreptul de a avea acces la:
  - datele personale prelucrate
  - o copie a datelor care nu poate să afecteze drepturile și libertățile altor persoane

Conform: expunerea (63), Art. (12), Art. (15)

Dreptul la ștergerea datelor (dreptul de a fi uitat)

Fără întârziere nejustificată, persoana vizată are dreptul la ștergerea datelor cu caracter personal care o vizează în următoarele cazuri:

- ✓ datele nu mai sunt necesare pentru îndeplinirea scopurilor
- ✓ persoana vizată își retrage consimțământul (dacă prelucrarea s-a făcut pe aceasta bază)
- ✓ persoana vizata se opune prelucrării și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea sau persoana vizată se opune în temeiul art. 21 alin. (2)
- ✓ datele cu caracter personal au fost prelucrate ilegal
- ✓ există o obligație legală pentru ștergerea datelor
- ✓ datele cu caracter personal au fost colectate în legatură cu oferirea de servicii ale societății informaționale

În cazul în care operatorul a făcut publice în alta parte datele cu caracter personal este obligat sa informeze operatorii care prelucrează datele cu caracter personal ca persoană vizată a solicitat ștergerea de către acești operatori a oricăror linkuri către datele respective sau a oricăror copii sau reproduceri ale acestor date cu caracter personal.

Excepții:

- ✓ exercitarea dreptului la libera exprimare și la informare
- ✓ respectarea unei obligații legale
- ✓ interesul public
- ✓ în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori in scopuri statistice
- ✓ pentru constatarea, exercitarea sau apărarea unui drept in instanță.

Conform: expunerea (65)-(66), art. (17)

Dreptul la restricționarea prelucrării

Persoana vizată are dreptul de a obține din partea operatorului restricționarea prelucrării în următoarele cazuri:

- ✓ persoana vizată contestă exactitatea datelor, pentru o perioadă care ii permite operatorului să verifice exactitatea datelor
- ✓ prelucrarea este ilegală, iar persoana vizată se opune ștergerii datelor cu caracter personal, solicitând în schimb restricționarea utilizării lor
- ✓ operatorul nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar persoana vizată i le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanță
- ✓ persoana vizată s-a opus prelucrării în conformitate cu art. 21 alin. (1), pentru intervalul de timp în care se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei

vizate în cazul în care prelucrarea a fost restricționată astfel de date cu caracter personal pot, cu excepția stocării, să fie prelucrate numai cu consimțământul persoanei vizate sau pentru constatarea, exercitarea sau apărarea unui drept în instanța sau pentru protecția drepturilor unei alte persoane fizice sau juridice sau din motive de interes public important al Uniunii sau al unui stat membru .

Conform: expunerea (67), art. (18)

Dreptul la portabilitatea datelor

Persoana vizată are dreptul:

- ✓ de a primi datele care o vizează și pe care le-a furnizat operatorului într-un format structurat, utilizat in mod curent și care poate fi citit automat
- ✓ de a transmite aceste date altui operator fără obstacole din partea operatorului sau direct de la un operator la altul, atunci când este fezabil din punct de vedere tehnic, atunci când prelucrarea se bazează pe consimțământ sau pe contract;
- ✓ prelucrarea este efectuată prin mijloace automate

Exercitarea acestui drept nu va aduce atingere drepturilor și libertăților altor persoane.

Conform: expunerea (68), art. (20)

Dreptul la opoziție și procesul decizional automatizat

Dreptul de a se opune prelucrării în orice moment

- ✓ persoana vizată are dreptul de a se opune, din motive legate de situația particulară în care se află, prelucrării în temeiul articolului 6 alineatul (1) litera (e) sau (f) sau al articolului 6 alineatul (1) a datelor cu caracter personal care o privesc, inclusiv creării de profiluri pe baza respectivelor dispoziții.
- ✓ operatorul nu mai prelucrează datele cu caracter personal cu excepția cazului în care operatorul demonstrează că are motive legitime si imperioase care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau ca scopul este constatarea, exercitarea sau apărarea unui drept în instanță.
- ✓ atunci când prelucrarea datelor cu caracter personal are drept scop marketingul direct:
  - persoana vizată are dreptul de a se opune în orice moment prelucrării în acest scop a datelor cu caracter personal care o privesc, inclusiv creării de profiluri, în măsura în care este legată de marketingul direct respectiv.
  - în cazul în care persoana vizată se opune prelucrării în scopul marketingului direct, datele cu caracter personal nu mai sunt prelucrate în acest scop.
- ✓ în scop de cercetare științifică sau istorică sau în scop statistic, persoana vizata, din motive legate de situația sa particulară, are dreptul de a se opune prelucrării datelor cu caracter personal care o privesc, cu excepția cazului în care prelucrarea este necesară din motive de interes public.
- ✓ dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri ce produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsura semnificativă.

Excepții:

- ✓ decizia este necesară pentru încheierea sau executarea unui contract între persoana vizată și un operator de date,
- ✓ decizia este autorizată prin dreptul Uniunii sau dreptul intern care se aplica operatorului și care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate
- ✓ decizia are la baza consimțământul explicit al persoanei vizate

În aceste cazuri operatorul de date pune în aplicare măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate, cel puțin dreptul acesteia de a obține intervenție umană din partea operatorului, de a-și exprima punctul de vedere și de a contesta decizia.

Conform: expunerea (69)-(70), art. (21)

Securitatea datelor cu caracter personal

Securitatea prelucrării

- ✓ măsuri tehnice si organizatorice adecvate
- ✓ pseudonimizare și criptare
- ✓ capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare
- ✓ capacitatea de a restabili disponibilitatea datelor cu caracter personal
- ✓ accesul la acestea în timp util în cazul în care are loc un incident de natura fizică sau tehnica
- ✓ un proces pentru testarea, evaluarea si aprecierea periodică ale eficacității măsurilor tehnice si organizatorice pentru a garanta securitatea prelucrării

Incidentul de securitate

Este o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal sau la accesul neautorizat la acestea.

Notificarea Autorității de Supraveghere în cazul unui incident de securitate

- ✓ în termen de cel mult 72 de ore de la data la care a luat cunoștință
- ✓ în cazul în care notificarea nu are loc in termen de 72 de ore aceasta este însoțită de o explicație motivată

Notificarea:

- descrie caracterul încălcării securității datelor cu caracter personal
- daca e posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză
- daca e posibil, categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză
- comunică numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații
- descrie consecințele probabile ale încălcării securității datelor cu caracter personal
- descrie măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal

- atunci când și în măsura în care nu este posibil să se furnizeze informațiile în același timp, acestea pot fi furnizate in mai multe etape, fără întârzieri nejustificate
- operatorul păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse. Aceasta documentație permite Autorității de Supraveghere să verifice conformitatea cu prezentul articol.

Notificarea persoanei vizate in cazul unui incident de securitate

- ✓ dacă este susceptibil sa genereze un risc ridicat pentru drepturile si libertățile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la incident
- ✓ într-un limbaj clar si simplu a caracterului incidentului.
  Conține cel puțin următoarele:
  - datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
  - consecințele probabile ale încălcării securității datelor cu caracter personal măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal

Conform: expunerea (74)-(77), (83), (85), (87), (88), art. (32), art. (33)

Consultarea prealabilă și evaluarea impactului asupra datelor cu caracter personal (DPIA)

În cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, trebuie efectuată o evaluare care conține cel puțin următoarele:

- ✓ o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator
- ✓ o evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri.
- ✓ o evaluare a riscurilor pentru drepturile si libertățile persoanelor vizate
- ✓ măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentului regulament, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor persoane interesate.

DPIA este necesară mai ales când avem următoarele situații:

- ✓ prelucrare automată, inclusiv crearea de profiluri, cu efect semnificativ asupra drepturilor persoanei
- ✓ prelucrare pe scara larga a unor categorii speciale de date, sau a unor date cu caracter personal privind condamnări penale și infracțiuni
- ✓ monitorizare sistematică pe scara larga a unei zone accesibile publicului

Operatorul se va consulta cu responsabilul cu protecția datelor atunci când efectuează DPIA.

Consultarea prealabilă

Operatorul consultă Autoritatea de Supraveghere înainte de prelucrare atunci când evaluarea impactului asupra protecției datelor prevăzută în DPIA indica faptul ca prelucrarea ar genera un risc ridicat în absența unor măsuri luate de operator pentru atenuarea riscului.

Conform: expunerea (75), (84), (89), (90)- (93), (94)- (96), art. (35), art. (36)

Responsabilul cu protecția datelor (DPO)

Operatorul și persoana împuternicită de operator desemnează, în mod obligatoriu, un responsabil cu protecția datelor în următoarele situații:

- ✓ prelucrarea este efectuata de o autoritate sau un organism public
- ✓ operatorul prelucrează numere unice naționale (legea 190/2018)
- ✓ activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau in operațiuni de prelucrare care, prin natura, domeniul de aplicare și/sau scopurile lor, necesită o monitorizare periodică și sistematică a persoanelor vizate pe scara largă
- ✓ activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scara larga a unor categorii speciale de date sau a unor date cu caracter personal privind condamnări penale și infracțiuni
- ✓ un grup de întreprinderi poate numi un responsabil cu protecția datelor unic cu condiția să fie accesibil în timp util de fiecare parte din grup

- DPO poate fi angajat sau externalizat
- datele de contact ale DPO trebuie transmise către Autoritatea de Supraveghere

DPO:

- ✓ operatorul se asigură că DPO este implicat in mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal
- ✓ are obligația de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale
- ✓ nu este demis sau sancționat de către operator sau de persoana împuternicită de operator pentru îndeplinirea sarcinilor sale (dar pentru neîndeplinire, da)
- ✓ răspunde direct în fața celui mai înalt nivel al conducerii

Atribuții :

1. Informarea și consilierea operatorului, sau a persoanei împuternicite de operator, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul prezentului regulament și al altor dispoziții de drept al Uniunii sau drept intern referitoare la protecția datelor
2. Monitorizarea respectării prezentului regulament, a altor dispoziții de drept al Uniunii sau de drept intern referitoare la protecția datelor și a politicilor
3. Alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare și auditurile referente.
4. Furnizarea de consiliere la cerere in ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia
5. Cooperarea cu Autoritatea de Supraveghere

6. Asumarea rolului de punct de contact pentru Autoritatea de Supraveghere privind aspectele legate de prelucrare

Conform: expunerea (91), (97), art. (35), art. (37), art. (38), art. (39)

Transferul datelor in țări din afara UE sau către organizații internaționale

Transferurile internaționale sunt permise în următoarele situații:

- ✓ transferuri în temeiul unei decizii privind caracterul adecvat al nivelului de protecție
- ✓ transferuri in baza unor garanții adecvate
- ✓ reguli corporative obligatorii
- ✓ derogări pentru situații specifice

În absența unei decizii privind caracterul adecvat al nivelului de protecție în conformitate cu art. 45 alin. (3) sau a unor garanții adecvate în conformitate cu art. 46, inclusiv a regulilor corporatiste obligatorii, un transfer sau un set de transferuri de date cu caracter personal către o țară terță sau o organizație internațională poate avea loc numai in una dintre condițiile următoare:

- ✓ persoana vizată și-a exprimat in mod explicit acordul cu privire la transferul propus, după ce a fost informată asupra posibilelor riscuri pe care astfel de transferuri le pot implica pentru persoana vizată ca urmare a lipsei unei decizii privind caracterul adecvat al nivelului de protecție si a unor garanții adecvate
- ✓ transferul este necesar pentru executarea unui contract intre persoana vizată și operator sau pentru aplicarea unor măsuri precontractuale adoptate la cererea persoanei vizate
- ✓ transferul este necesar pentru încheierea unui contract sau pentru executarea unui contract încheiat în interesul persoanei vizate între operator si o alta persoana fizică sau juridică
- ✓ transferul este necesar din considerente importante de interes public
- ✓ transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanța
- ✓ transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale altor persoane, atunci când persoana vizata nu are capacitatea fizica sau juridică de a-și exprima acordul
- ✓ transferul se realizează dintr-un registru care, potrivit dreptului Uniunii sau al dreptului intern, are scopul de a furniza informații publicului si care poate fi consultat fie de public in general, fie de orice persoana care poate face dovada unui interes legitim, dar numai in măsura în care sunt îndeplinite condițiile cu privire la consultare prevăzute de dreptul Uniunii sau de dreptul intern în acel caz specific.

Conform: expunerea (101)-(110), art. (35), art. (44)-(50)

Sancțiuni si remediere

Drepturile persoanei vizate:

- ✓ dreptul persoanei vizate de a depune o plângere la Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, în cazul în care consideră că prelucrarea datelor cu caracter personal care o vizează încalcă prezentul regulament
- ✓ dreptul la despăgubire al persoanei vizate din partea operatorului sau a persoanei împuternicite
- ✓ dreptul la o cale de atac judiciară eficientă împotriva unui operator sau unei persoane împuternicite de operator

Sancțiunile:

- ✓ avertismentul
- ✓ amenda contravențională de până la 10 000 000 EUR sau, în cazul unei întreprinderi, de până la 2% din cifra de afaceri pentru încalcarea:
  - obligațiilor operatorului și ale persoanei împuternicite de operator in conformitate cu articolele 8, 11, 25-39, 42 si 43
  - obligaților organismului de certificare în conformitate cu articolele 42 si 43;
  - obligațiilor organismului de monitorizare în conformitate cu articolul 41 alineatul (4).
- ✓ amenda contravențională de pana la 20 000 000 EUR sau, în cazul unei întreprinderi, de până la 4% din cifra de afaceri pentru încălcarea:
  - principiilor de baza pentru prelucrare, inclusiv condițiile privind consimțământul, in conformitate cu articolele 5, 6, 7 si 9
  - drepturilor persoanelor vizate in conformitate cu articolele 12-22
  - transferurilor de date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională, în conformitate cu articolele 44-49
  - oricăror obligații adoptate în temeiul legislației naționale
  - nerespectării unui ordin sau a unei limitări temporare sau definitive asupra prelucrării, sau a suspendării fluxurilor de date, emisă de către Autoritatea de Supraveghere
  - încălcării unui ordin emis de Autoritatea de Supraveghere in conformitate cu articolul 58 alineatul (2)

Stabilirea sancțiunilor

Atunci când se ia decizia dacă se va da un avertisment sau o amendă, inclusiv cuantumului acesteia din urmă, se vor avea in vedere următoarele:

- natura, gravitatea și durata încălcării, ținându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum și de numărul persoanelor vizate afectate si de nivelul prejudiciilor suferite de acestea
- dacă încălcarea a fost comisa intenționat sau din neglijență
- acțiunile întreprinse pentru reducerea prejudiciului persoanei vizate
- gradul de responsabilitate
- eventualele încălcări anterioare relevante
- gradul de cooperare cu Autoritatea de Supraveghere pentru a remedia încălcarea și a atenua posibilele efecte negative ale încălcării
- categoriile de date cu caracter personal afectate de încălcare
- modul în care încălcarea a fost adusă la cunoștința autorității de supraveghere, în special dacă și în ce măsură operatorul sau persoana împuternicită de operator a notificat încălcarea
- aderarea la coduri de conduită aprobate
- orice alt factor agravant sau atenuant aplicabil circumstanțelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect de pe urma încălcării

Conform: expunerea (141)-(152), art. (77)-(84)