BAZA LEGALĂ

La nivel comunitar:

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)**

pe scurt: General Data Protection Regulation- GDPR

data aplicării: 25 mai 2018

În România:

Proiect de lege**- Senat-**

http://www.cdep.ro/pls/proiecte/upl_pck2015.proiect?cam=2&idp=16976

https://www.senat.ro/legis/lista.aspx?nr_cls=b240&an_cls=2018

Ghiduri ale Grupului de lucru- (Working Party)**- în baza articolului 29 din Regulament -pot fi consultate în limba engleză, iar o parte dintre acesta, sunt disponibile și în limba romana.**

Grupul de lucru

Este un organism european independent, cu caracter consultativ, format din reprezentanții autorităților naționale pentru protecția datelor din statele membre ale Uniunii Europene, reprezentanții autorităților create pentru instituțiile și organismele comunitare, precum și reprezentanți ai Comisiei Europene.

EXEMPLE DE DATE CU CARACTER PERSONAL

„date cu caracter personal" **înseamnă orice informații 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 identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale; *-art. 4 punctul 1 din GDPR***

- -numele
- -adresa
- -data nașterii
- -nr de identificare-CNP
- -cetățenia
- -naționalitatea
- -orientarea sexuală
- -orientarea politică
- -orientarea religioasă
- -date medicale
- -date biometrice
- -imaginea
- -date care privesc localizarea persoanei
- -adresa de email
- -nr de cont bancar
- -informații legate de contravenții și infracțiuni

CUM ȘTIU DACĂ PRELUCREZ DATE CU CARACTER PERSONAL?

Prelucrarea datelor cu caracter personal reprezintă *orice operațiune care privește datele cu caracter personal.*

Exemple de prelucrare a datelor cu caracter personal:

-colectarea
-înregistrarea
-organizarea
-structurarea
-stocarea
-păstrarea
-adaptarea ori modificarea
-extragerea
-consultarea
-utilizarea
-divulgarea către terți prin transmitere, diseminare sau punere la dispoziție în orice alt mod
-alinierea
-combinarea
-restricționarea
-ștergerea
-distrugerea datelor cu caracter personal.

ART.1 Regulament

Prezentul regulament se aplică prelucrării datelor cu caracter personal, efectuată total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor.

Dacă în activitatea dumneavoastră interacționați cu persoane fizice, indiferent de calitatea acestora (salariați, clienți, parteneri, etc.) prelucrați date cu caracter personal și trebuie sa va Conformați GDPR.

CE OBLIGAȚII AM ÎNAINTE DE INTRAREA ÎN VIGOARE A REGULAMENTULUI?

1. Identificarea categoriilor de date cu caracter personal prelucrate

Primul pas constă în identificarea tuturor categoriilor de date personale prelucrate de către toate departamentele unei societăți, precum și în identificarea tuturor activităților de prelucrare.

Se poate porni de la organigrama societății.

2. Stabilirea scopurilor în care are loc prelucrarea, respectiv pentru ce sunt prelucrate datele.

Exemple:

- încheierea și executarea contractului individual de munca,
-completarea REVISAL,
-plata salariului prin virament bancar,
-emiterea unor facturi, pentru oferirea unor servicii, etc.

3. Stabilirea temeiului în baza căruia are loc prelucrarea, pentru fiecare categorie de date în parte.

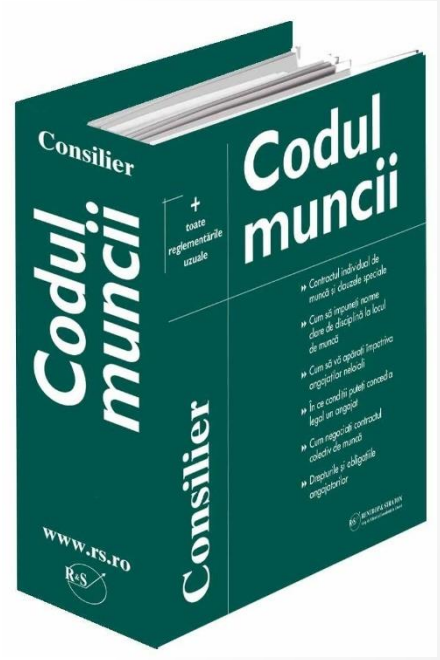
Exista 4 mari categorii de temeiuri în baza cărora operatorii pot prelucra date:

- **îndeplinirea unei *obligații legale* a societății**
- ***interesul legitim* urmărit de către societate sau de către un terț**
- ***executarea unui contract* la care persoana vizată este parte sau pentru a face *demersuri, la cererea persoanei vizate*, înainte de încheierea unui contract**
- ***consimțământul* sau acordul persoanei vizate.**

❑ Îndeplinirea unei obligații legale a societății

- obligație care rezultă dintr-o lege

Exemplu: solicitarea numelui, a prenumelui și a adresei în vederea încheierii Contractului Individual de Muncă este o obligație legală a societății Angajatoare - art.13 și art.14 Codul Muncii.



❑ Interesul legitim urmărit de către societate sau de către un terț

Exemplu: instalarea unor camere de luat vederi la locul de muncă poate să aibă la bază interesul legitim al societății angajatoare

- **Executarea unui contract la care persoana vizată este parte sau pentru a face demersuri, la cererea persoanei vizate, înainte de încheierea unui contract**

Exemplu: solicitarea datelor bancare de la un angajat pentru a efectua plata salariului prin transfer bancare ca temei executarea unui contract, respectiv Contractul Individual de Muncă.

❑ Consimțământul sau acordul persoanei vizate

Consimțământul persoanei vizate poate fi folosit ca temei în condiții mai restrictive decât în prezent.

El trebuie să fie solicitat într-o forma accesibilă oricărei persoane, iar retragerea lui trebuie să se facă la fel de simplu cum a fost dat.

Exemplu: daca o persoana își dă consimțământul prin bifarea unei căsuțe, retragerea consimțământului trebuie să se facă în aceeași maniera

Consimțământul:

- -trebuie sa fie **liber**, nu poate fi condiționat
- -trebuie să fie **specific** dat pentru fiecare scop al prelucrării în parte;
- exemplu: dacă o persoană își dă consimțământul să îi folosiți adresa de email pentru a-i trimite un newsletter, nu puteți să îi furnizați adresa de email unui alt operator, pentru ca și acesta să îi transmită un newsletter.
- -trebuie să fie **informat**; persoanei vizate trebuie să i se explice în ce scop îi vor fi folosite datele și care sunt consecințele acestei utilizări, precum și ce drepturi are
- **-toate explicațiile trebuie sa fie date într-un limbaj accesibil**

DATA PROTECTION IMPACT ASSESSMENTS -DPIA (EVALUAREA IMPACTULUI) CUNOSCUT ȘI SUB NUMELE DE ”PIA”

Una dintre practicile recomandate pentru evaluarea riscurilor și impactului pe care îl poate avea prelucrarea datelor personale este efectuarea unui studiu de impact asupra protecției sau confidențialității datelor.

De regulă, o analiză a riscului și a impactului pe care îl presupune prelucrarea unor date personale trebuie să fie făcută atunci când sunt introduse tehnologii noi, dar și atunci când este posibil ca prelucrarea să conducă la un risc ridicat pentru drepturile și libertățile persoanelor.

Este absolut necesară în cazul în care există o prelucrare automată și prelucrarea unor categorii speciale de date pe scară largă.

Ce informații ar trebui să conțină DPIA?

- orice evaluare de impact trebuie să conțină:
- descrierea operațiunilor de prelucrare și a scopurilor, inclusiv (dacă este cazul) a intereselor legitime urmărite de operator;
- evaluarea necesității și proporționalității procesării în raport cu scopul;
- evaluarea riscurilor pentru persoane fizice;
- măsurile luate pentru a reduce riscul, inclusiv securitatea și pentru a demonstra că vă conformați;

Dacă prelucrarea datelor presupune un grad de risc ridicat, se impune consultarea autorității de supraveghere înainte de prelucrare, iar aceasta oferă consiliere în scris solicitantului și, după caz, persoanei împuternicite de acesta, în cel mult opt săptămâni de la primirea cererii de consultare.

4. Stabilirea datei la care încetează prelucrarea sau a criteriilor în funcție de care se stabilește această dată

5. Minimizarea – nu vor mai fi prelucrate acele categorii de date pentru care nu a fost identificat un temei și care nu sunt necesare

6. Updatare politici și documente interne, precum și contracte- contractele individuale de munca și contractele cu colaboratorii

7. Întocmirea registrului operațiunilor de prelucrare

8. Redactarea modelului de obținere a consimțământului și obținerea noului consimțământ

9. Redactarea modelului de informare a persoanei vizate - Privacy Notice

10. Discuții și training cu Departamentul IT pentru implementarea procedurilor

11. Instruirea angajaților

BREȘA DE SECURITATE

Obligații ale operatorului în cazul unei breșe de securitate

- **raportarea incidentului către Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal în termen de 72 de ore de la data la care a luat cunoștința de el.**

  Orice întârziere trebuie să fie motivata în scris.

Ce trebuie sa conțină informarea adresata ANSPDCP?

- - natura breșei, inclusiv numărul de persoane afectate și numărul de date cu caracter personal afectate.
- - datele de contact ale responsabilului cu protecția datelor (dacă organizația ta a desemnat unul).
- -o descriere ale posibilelor consecințe ale breșei dar și o descriere a măsurilor pe care le veți lua pentru remedierea situației.

- **informarea persoanei vizate dacă încălcarea securității este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile sale.**

Modelul de notificare va fi disponibil pe site-ul ANSPDCP.

Salvarea ar putea veni însă de la metodele de securitate folosite. Dacă datele furate sunt criptate și, astfel, nu pot fi accesate de către cei care le-au furat sau găsit, obligația de a informa persoanele afectate nu mai subzistă.

Deoarece termenele de raportare sunt foarte scurte, este important ca, la nivelul societății să existe o procedură de raportare internă a unor astfel de incidente.

- https://www.youtube.com/watch?v=opRMrEfAIiI

DREPTURILE PERSOANEI VIZATE

1. **dreptul de a avea acces la datele sale:** poate solicita să i se comunice categoriile de date cu caracter personal care îi sunt prelucrate, scopul în care are loc prelucrarea, destinatarii cărora le-au fost sau vor fi comunicate, perioada pentru care se preconizează că vor fi stocate sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă; existența unui proces decizional automatizat incluzând crearea de profiluri

2. **dreptul de a solicita rectificarea datelor**: în situația în care exista erori cu privire la datele care îi sunt prelucrate, are posibilitatea de a solicita corectarea lor; în cazul în care datele sunt incomplete, poate solicita completarea lor

3. **dreptul de a solicita restricționarea prelucrării datelor:** are dreptul de a solicita restricționarea prelucrării datelor în următoarele situații:

-dacă a contestat exactitatea datelor, pentru o perioadă care îi permite operatorului să verifice exactitatea datelor;

-dacă 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;

- s-a opus prelucrării pentru intervalul de timp în care se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate.

DREPTURILE PERSOANEI VIZATE

4. dreptul de a solicita ștergerea datelor: poate solicita ștergerea datelor prelucrate, dacă datele nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate , dacă și-a retras consimțământul și nu există niciun alt temei juridic pentru prelucrarea; dacă se opune prelucrării și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea; datele cu caracter personal au fost prelucrate ilegal; datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale conform dreptului intern sau dreptului comunitar.

Acest drept nu poate fi exercitat dacă datele sunt necesare pentru exercitarea dreptului la liberă exprimare și la informare; pentru respectarea unei obligații legale care prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului sau pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este învestit operatorul; din motive de interes public în domeniul sănătății publice, în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice sau pentru constatarea, exercitarea sau apărarea unui drept în instanță.

5. dreptul de a solicita transferul datelor: poate solicita transferul datelor către un alt operator dacă prelucrarea are la baza consimțământul sau și prelucrarea este una automata

DREPTURILE PERSOANEI VIZATE

6. dreptul de a va opune prelucrării: are dreptul să se opună prelucrării datelor dacă ele privesc marketingul direct. Totodată, se poate opune prelucrării, cu excepția cazului în care operatorul demonstrează că are motive legitime care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanță.

7. **dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automatizată a datelor. Acest drept nu poate fi exercitat atunci când prelucrarea este necesară pentru încheierea sau executarea unui contract între persoana vizată și un operator de date; este autorizată prin dreptul Uniunii sau dreptul intern care se aplică operatorului și care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate; sau are la bază consimțământul explicit al persoanei vizate.**

AMENZI

- **amenzi administrative de până la 10 000 000 EUR sau, în cazul unei întreprinderi, de până la 2 % din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare, pentru încălcarea unor obligații cum sunt cele privitoare la:**
  - obținerea consimțământul copiilor în legătură cu serviciile societății informaționale,
  - păstrarea evidenței activității de prelucrare,
  - notificarea în cazul breșelor de securitate, etc.

- **amenzi administrative de până la 20 000 000 EUR sau, în cazul unei întreprinderi, de până la 4 % din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare pentru:**

-încălcarea principiilor de bază pentru prelucrare, inclusiv condițiile privind consimțământul, a drepturilor persoanelor vizate, a dispozițiilor cu privire la transferurile de date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională, etc.

SUPERHEROES

Vă mulțumim!

Sursa foto: https://www.gdprsuperheroes.com/