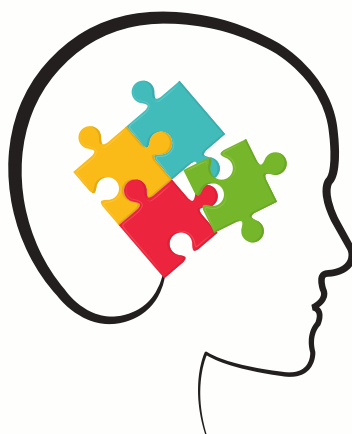


GDPR

pe înțelesul tău



ghid pentru
implementare

Ruxandra Sava

CIPP/E

GDPR explicat pe înțelesul tău

Ruxandra Sava, CIPP/E

Cuprins

Capitolul I. Introducere în Regulamentul (EU) nr. 679/2016	4
1.1. Regulamentul (EU) 679/2016.....	4
1.1. Ce aduce nou Regulamentul (EU) 679/2016?	6
Capitolul 2. Noțiuni introductive	7
2.1. Ce sunt datele cu caracter personal?	7
2.2. Ce sunt categoriile speciale de date?	11
2.3. Datele anonimizate și datele pseudonimizate	13
2.4. Operatorul și persoana împuternicită de operator.....	15
Persoana împuternicită de operator.....	18
Relația dintre operator și persoana împuternicită de operator	20
2.6. Persoana vizată	24
Capitolul 3. Principiile prelucrării datelor cu caracter personal	25
3.2. Legalitate, echitate și transparență	25
3.3. Limitări legate de scop.....	29
3.4. Reducerea la minimum a datelor	30
3.5. Exactitate	31
3.6. Limitări legate de stocare.....	31
3.7. Integritate și confidențialitate	32
Capitolul 4. Legalitatea prelucrării	34

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

4.1.	Introducere	34
4.2.	Legalitatea prelucrării categoriilor obișnuite de date cu caracter personal	34
	Consimțământul	35
	Contractul	39
	Obligația legală	40
	Interesul vital	41
	Interesul public	41
	Interesul legitim	41
	Cum se alege temeiul juridic corect pentru prelucrare?	44
4.3.	Legalitatea prelucrării categoriilor speciale de date	44
Capitolul 5. Drepturile persoanei vizate		48
5.1.	Introducere	48
5.2.	Dreptul la informare	50
5.3.	Dreptul de acces	58
5.5.	Dreptul la ștergerea datelor	59
5.6.	Dreptul la restricționarea prelucrării	61
5.7.	Dreptul la portabilitatea datelor	62
5.8.	Dreptul la opoziție	63
5.9.	Procesul decizional individual automatizat, inclusiv crearea de profiluri	63
Capitolul 6. Incidentele de securitate		66
	<i>Procedura de notificare a incidentelor de securitate</i>	67
	<i>Organizația va decide dacă va notifica ANSPDCP sau nu</i>	67
	<i>Cum se notifică Autoritatea de Supraveghere</i>	68
Capitolul 7. Securitatea prelucrării		72
Capitolul 8. Responsabilitatea		79
8.1.	Evidența activităților de prelucrare	79
8.2.	Evaluarea impactului asupra protecției datelor (DPIA)	80

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

8.3. Responsabilul cu protecția datelor	81
Capitolul 9. Transferurile internaționale	90
Transferurile în temeiul unei decizii privind caracterul adecvat al nivelului de protecție.....	90
Transferuri în baza unor garanții adecvate	91
Reguli corporatiste obligatorii	91
Derogări pentru situații specifice	92

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Capitolul I. Introducere în Regulamentul (EU) nr. 679/2016

1.1. Regulamentul (EU) 679/2016¹

Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal este un drept fundamental. Articolul 8 alineatul (1) din [Carta drepturilor fundamentale a Uniunii Europene](#)² („Carta”) și articolul 16 alineatul (1) din [Tratatul privind funcționarea Uniunii Europene](#)³ („TFUE”) prevăd dreptul oricărei persoane la protecția datelor cu caracter personal care o privesc.⁴

Evoluțiile tehnologice rapide și globalizarea au generat noi provocări pentru protecția datelor cu caracter personal. Amploarea colectării și a schimbului de date cu caracter personal a crescut în mod semnificativ. Tehnologia permite atât societăților private, cât și autorităților publice să utilizeze date cu caracter personal la un nivel fără precedent în cadrul activităților lor.⁵

La nivelul Uniunii Europene, până în prezent, principalul instrument juridic al UE pentru protecția datelor a fost Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995⁶ privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (**„Directiva privind protecția datelor”**).

Directiva 95/46/CE a fost transpusă intern în România prin [Legea nr. 677/2001](#) pentru

¹ Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) a fost publicat în Jurnalul Oficial al Uniunii Europene nr. L111/04.05.2016 și poate fi accesat [aici](#).

² Carta drepturilor fundamentale a Uniunii Europene a fost publicată în Jurnalul Oficial al Uniunii Europene nr. C83/30.02.2010 și poate fi accesată [aici](#).

³ Tratatul privind funcționarea Uniunii Europene (versiune consolidată) a fost publicat în Jurnalul Oficial al Uniunii Europene nr. C326/26.10.2012 și poate fi accesat [aici](#).

⁴ Par. (1) Preambul Regulamentul (EU) 679/2016.

⁵ Par. (6) Preambul Regulamentul (EU) 679/2016.

⁶ Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date a fost publicată în Jurnalul Oficial al Uniunii Europene nr. L281/23.11.1995 și poate fi accesată [aici](#).

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.⁷

Deși Directiva 95/46/CE a introdus mecanisme solide privind protecția datelor cu caracter personal, aceasta a avut câteva dezavantaje.

Comaniile de azi prelucrează date în moduri care nu puteau fi prevăzute în anul 1995, atunci când Directiva 95/46/CE a fost adoptată. În acea perioadă nu exista Google. Google a fost fondat abia în 1998. Tot pe atunci, nu aveam conturi de Facebook, nu făceam cumpărături online, iar locația noastră nu era urmărită de aproape toate aplicațiile cărora, uneori, din neatenție, le dăm permisiunea să facă acest lucru.

Directiva a fost transpusă diferit în statele membre și au existat bariere cu privire la libera circulație a datelor.

Tehnologia evoluează rapid, iar legislația trebuie să țină pasul cu ea. În ajunul tranziției către era digitală, la nivel european, s-a decis că actuala legislație nu poate ține pasul cu evoluția tehnologică și nu oferă suficientă protecție persoanelor fizice. Astfel, s-a decis adoptarea unui Regulament European, care să armonizeze legislația în domeniul protecției datelor cu caracter personal în fiecare stat membru.

Spre deosebire de Directivă, Regulamentul (EU) 679/2016 („**Regulamentul**”, „**RGPD**” sau „**GDPR**”) se va aplica direct în toate statele membre începând cu data de 25 mai 2018 și reprezintă o evoluție în domeniul datelor cu caracter personal.

Regulamentul este construit pe legislația actuală, dar oferă mai multă protecție și control persoanelor fizice și mai multe obligații companiilor. Regulamentul are o abordare adaptată la secolul 21 și la evoluțiile preconizate în tehnologie: internetul lucrurilor, inteligența artificială, machine learning.

Cu alte cuvinte, unul dintre scopurile primordiale ale GDPR este să ofere protecție persoanele fizice cu privire la datele lor personale în timpurile care vor urma: (IoT) -

⁷ Legea nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date a fost publicată în Monitorul Oficial nr. 790 din 12 decembrie 2001.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

internet of things (era în care frigiderul va ține legătura cu supermarketul, iar mașinile autonome vor fi conectate la rețeaua rutieră), inteligența artificială sau etapa în care vom accepta existența roboților printre noi, iar cei mai inteligenți dintre ei vor lua decizii în privința noastră, iar noi, probabil, le vom oferi drepturi.

1.1. Ce aduce nou Regulamentul (EU) 679/2016?

Printre schimbările aduse de RGDP se numără:

- **Extinderea domeniului de aplicare teritorială;**
 - ✚ RGDPD **protejează drepturile tuturor persoanelor aflate pe teritoriul UE**, indiferent de poziționarea geografică a operatorului de date;
 - ✚ RGPD **extinde sfera de aplicare și asupra operatorilor de date stabiliți în afara UE**, în măsura în care bunurile și/sau serviciile acestora sunt adresate (și) persoanelor aflate pe teritoriul UE;
- **Noi drepturi:** dreptul la ștergerea datelor sau dreptul de a fi uitat și dreptul la portabilitatea datelor;
- Obligația desemnării, în unele cazuri, a unui **responsabil cu protecția datelor**;
- **Evaluarea impactului** prelucrării datelor cu caracter personal;
- Prevederi speciale referitoare la **prelucrarea datelor personale aparținând copiilor**;
- Reguli noi privind **transparența față de persoana vizată**;
- **Sanțiuni severe** de până la 4% din cifra de afaceri sau 20.000.000, oricare din ele este mai mare.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Capitolul 2. Noțiuni introductive

2.1. Ce sunt datele cu caracter personal?

Pe scurt:

- Datele cu caracter personal sunt orice informații care se referă la o persoană identificată sau care poate fi identificată, denumită „**persoană vizată**”;
- O persoană poate fi identificată dacă se pot obține informații suplimentare cu privire la ea pentru a o identifica;
- Datele cu caracter personal trebuie să se refere la o persoană fizică în viață;
- Datele publice pot fi date cu caracter personal, cu excepția situației în care au fost făcute publice de către persoana vizată în mod direct, fără dubiu;
- Există mai multe categorii de date:
 - **datele obișnuite** (ca de exemplu numele, adresa de e-mail, domiciliul etc), majoritatea datelor intrând în această categorie și există categorii speciale de date, și
 - așa-numitele **date sensibile** (datele biometrice, datele medicale, CNP-ul etc), care au un regim special și pot fi prelucrate respectând anumite condiții stricte.
- **Anonimizarea** datelor înseamnă că datele nu mai conțin niciun element de identificare;
- **Pseudonimizarea** datelor înseamnă că datele sunt înlocuite cu un cod.

👉 Datele anonimizate nu mai sunt date cu caracter personal, în schimb datele pseudonimizate sunt în continuare date cu caracter personal.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

☞ Regulamentul definește datele cu caracter personal drept **„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”**.⁸

GDPR **extinde definiția datelor cu caracter personal**. Acest lucru poate include acum identificatori online și chiar date genetice și biometrice, cum ar fi amprente digitale, scanarea retinei, recunoașterea vocală și recunoașterea facială. Parolele sunt, de asemenea, considerate date personale în cadrul GDPR.⁹

Utilizarea sintagmei **„orice informație”** a fost folosită în mod intenționat de legiuitorul european, pentru a nu exclude, din sfera de protecție, anumite categorii de date cu caracter personal.

Curtea de Justiție a Uniunii Europene a decis, în cauza [C-582/14](#) faptul că inclusiv o adresă IP dinamică poate fi, în anumite circumstanțe, o dată cu caracter personal.

Asemănător, în Cauza [C-434/16](#), CJUE a decis că foaia de examen a unui candidat se încadrează în conceptul de date cu caracter personal.

Grupul de Lucru Art. 29 recomandă, pentru a identifica dacă o anumită informație este dată cu caracter personal, a se lua în calcul patru piloni:¹⁰

- orice informație;
- care se referă la;

⁸ Art. 4 pct. 1 din Regulamentul (EU) 679/2016.

⁹ GDPR for Dummies. Editat de Meta Compliance Group, ce poate fi accesat [aici](#).

¹⁰ Opinia 4/2007 a Grupului de Lucru Art. 29, adoptată pe 20 iunie 2017, ce poate fi accesată [aici](#).

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

[#wemakeGDPRsimple](#)

- o persoană fizică identificată sau identificabilă.

„Orice informație”

Domeniul este atât de vast încât nu va exista niciodată o listă exhaustivă a datelor cu caracter personal. Acestea includ numele, adresa de e-mail, datele biometrice (imagini faciale, amprente), CNP, locația unei persoane, ocupația, sexul etc. Absolut orice informație.

Datele trebuie să se refere la persoanele fizice în viață. **Regulamentul nu se aplică și datelor privind persoanele decedate.**¹¹

Informațiile pot fi atât obiective, cât și subiective:

☞ Exemplu: Evaluarea performanței unui angajat la locul de muncă reprezintă o informație cu caracter personal, chiar dacă reflectă doar opinia personal a supervisorului, ca de exemplu „Angajatul X este mereu obosit” sau „Angajatul X nu este dedicat muncii sale.”

Informațiile sunt date cu caracter personal, indiferent că se referă la viața privată sau viața profesională a individului.¹² De exemplu, adresa de e-mail de serviciu intră în categoria de date cu caracter personal.

Paragraful 30 din Preambulul Regulamentului spune faptul că inclusiv adresele IP, identificatorii cookie sau alți identificatori precum etichetele de identificare prin frecvențe radio pot fi date cu caracter personal, deoarece pot lăsa urme, care, combinate cu alte informații primite de servere pot conduce către identificarea persoanelor, prin

¹¹ <https://www.facebook.com/legalup.ro/?ref=search>, Ruxandra Sava, 5 ianuarie 2018

¹² A se vedea Hotărârea CEDO din 16 februarie 2000 în cauza Amann/Elveția, nr. 27798/95, punctul 65.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

crearea de profiluri.¹³

„Care se referă la”

Pentru a intra în sfera datelor cu caracter personal, informațiile trebuie să se refere la o persoană fizică în viață. În unele cazuri informațiile cu privire la obiecte, fapte sau procese pot fi date cu caracter personal dacă există o legătură strânsă între acestea și persoana fizică, *de exemplu*, mașina colegului Mihai, telefonul clientului Andrei, parola utilizatorului mihai.andrei78.

Dacă anumiți factori exteriori, cum ar fi obiectele, procesele, evenimentele, faptele pot conduce la evalua sau analiza un individ într-un anumit mod, ar trebui să se considere a fi date cu caracter personal.¹⁴

„O persoană fizică identificată sau identificabilă.”

Situația datelor referitoare la persoane fizice identificate este clară (domiciliul angajatului X, CNP-ul clientului Y, e-mail-urile abonaților X,Y,Z).

Ce se întâmplă, însă, dacă avem date care nu se referă la o persoană fizică deja identificată? Sunt ele date personale?

Pot fi. Dacă există mijloace care pot conduce către identificarea persoanei. Aceste mijloace trebuie să țină cont atât de tehnologia actuală, cât și de cea care va fi, în mod rezonabil, dezvoltată în viitor.

Identificarea persoanei se poate realiza prin nume. Însă, simplul fapt că nu știm numele unei persoane, nu înseamnă că aceasta nu poate fi identificată. Cei mai mulți dintre noi nu știm numele tuturor vecinilor, însă îi putem identifica. Pentru identificare, ne

Preambul (30) din Regulamentul (EU) 679/2016: „Persoanele fizice pot fi asociate cu identificatorii online furnizați de dispozitivele, aplicațiile, instrumentele și protocoalele lor, cum ar fi adresele IP, identificatorii cookie sau alți identificatori precum etichetele de identificare prin frecvențe radio. Aceștia pot lăsa urme care, în special atunci când sunt combinate cu identificatori unici și alte informații primite de servere, pot fi utilizate pentru crearea de profiluri ale persoanelor fizice și pentru identificarea lor.”

¹⁴ Opinia 4/2007 a Grupului de Lucru Art. 29.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

raportăm, potrivit Regulamentului la „*un număr de identificare ori la unul sau la mai mulți factori specifici identității sale fizice, fiziologice, psihice, economice, culturale sau sociale*”

Cu alte cuvinte, dacă avem o informație care nu este atribuită unei persoanei, însă putem folosi informații suplimentare (prin orice mijloace) pentru a identifica persoana respectiva, vorbim de date cu caracter personal.

☞ *Exemplu: „Datele referitoare la salariile într-o companie nu sunt, în general, date cu caracter personal. Aceste date se pot regăsi, fără probleme, în anunțurile de recrutare. Însă, dacă într-o companie există un singur angajat pe un anumit post, salariul aferent aceluia post este o informație cu caracter personal care se referă la singurul angajat care ocupa respectivul post.”¹⁵*

2.2. Ce sunt categoriile speciale de date?

Pe scurt

- ✚ GDPR include în sfera categoriei speciale datele care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice, apartenența la sindicate, datele genetice, datele biometrice pentru identificarea unică a unei persoane fizice, datele privind sănătatea sau datele privind viața sexuală sau orientarea sexuală ale unei persoane fizice.
- ✚ Datele genetice și cele biometrice sunt incluse în această categorie dacă sunt prelucrate în așa fel încât identifică în mod unic o persoană.
- ✚ Categoriile speciale de date au un regim special, regula fiind aceea că sunt interzise a fi prelucrate, existând totuși câteva excepții.
- ✚ Datele privind condamnările penale și infracțiunile nu sunt incluse în această

¹⁵ A se vedea în acest sens și postarea de pe Facebook a paginii LegalUp din data de 5 ianuarie 2018, ce poate fi accesată [aici](#).

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

categorie, dar condițiile pentru prelucrare sunt similare.¹⁶

Există anumite categorii de date personale, care, dacă sunt prelucrate, pot prezenta un risc pentru individ. Aceste date au un regim special, necesită o protecție sporită și pot fi prelucrate doar în anumite condiții stricte.

Categoriile speciale de date sunt următoarele:

- Datele care dezvăluie *originea rasială sau etnică*;
- Datele care dezvăluie *opiniile politice*;
- Datele care dezvăluie *confesiunea religioasă sau convingerile filozofice*;
- Datele care dezvăluie *apartenența la sindicate*;
- *Datele genetice*¹⁷ și *datele biometrice*¹⁸ pentru identificarea unică a unei persoane fizice;
- *Datele privind sănătatea*¹⁹; și

¹⁶ ICO's Guide to the General Data Protection Regulation (GDPR), ce poate fi accesat [aici](#).

¹⁷ Art. (4) pct. 13 din Regulamentul (EU) 679/2016: „date genetice” înseamnă datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea persoanei respective și care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;”

¹⁸ Art. (4) pct. 14 din Regulamentul (EU) 679/2016: „date biometrice” înseamnă o date 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;”

¹⁹ Par. (35) Preambulul Regulamentului (EU) 679/2016: „Datele cu caracter personal privind sănătatea ar trebui să includă toate datele având legătură cu starea de sănătate a persoanei vizate care dezvăluie informații despre starea de sănătate fizică sau mentală trecută, prezentă sau viitoare a persoanei vizate. Acestea includ informații despre persoana fizică colectate în cadrul înscrierii acesteia la serviciile de asistență medicală sau în cadrul acordării serviciilor respective persoanei fizice în cauză, astfel cum sunt menționate în Directiva 2011/24/UE a Parlamentului European și a Consiliului (1); un număr, un simbol sau un semn distinctiv atribuit unei persoane fizice pentru identificarea singulară a acesteia în scopuri medicale; informații rezultate din testarea sau examinarea unei părți a corpului sau a unei substanțe corporale, inclusiv din date genetice și eșantioane de material biologic; precum și orice informații privind, de exemplu, o boală, un handicap, un risc de îmbolnăvire, istoricul medical, tratamentul clinic sau

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

[#wemakeGDPRsimple](#)

- *Datele privind viața sexuală sau orientarea sexuală;*

Având în vedere regimul similar, vom include în această categorie și datele privitoare la condamnările penale sau infracțiunile.

☞ *Exemplu: În cauza Bodil Lindqvist⁶⁶, CJUE a declarat că „precizarea faptului că o persoană s-a rănit la picior și lucrează cu fracțiune de normă pe motive medicale constituie date cu caracter personal referitoare la starea de sănătate, în sensul articolului 8 alineatul (1) din Directiva 95/46.”²⁰*

👉 În expunerea de motive, Regulamentul precizează că **prelucrarea fotografiilor nu ar trebui să fie considerată prelucrare de categorii speciale**, deoarece fotografiile nu intră în sfera datelor biometrie decât atunci când sunt prelucrate printr-un mijloc tehnic specific care permite identificarea unică a unei persoane fizice.²¹

2.3. Datele anonimizate și datele pseudonimizate

Pe scurt

- 📌 Datele **nu trebuie stocate mai mult decât este necesar**. Odată ce s-a împlinit perioada stocării, datele pot fi stocate doar dacă au fost anonimizate complet.
- 📌 GDPR încurajează pseudonimizarea datelor, fiind unul dintre cele mai importante mijloace de protecție.
- 📌 Pseudonimizarea se poate obține, spre exemplu, prin înlocuirea unui element de identificare un un cod.

Datele anonimizate

Datele sunt anonimizate, atunci când orice element de identificare dispăre. Dacă un

starea fiziologică sau biomedicală a persoanei vizate, indiferent de sursa acestora, ca de exemplu, un medic sau un alt cadru medical, un spital, un dispozitiv medical sau un test de diagnostic in vitro.”

²⁰ Hotărârea CJUE din 6 noiembrie 2003 în cauza Bodil Lindqvist, C-101/01, punctul 51.

²¹ Par. (51) din Preambulul Regulamentului (EU) 679/2016

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

element rămas poate servi, singur sau împreună cu altele, la reidentificarea persoanei, atunci anonimizarea nu a fost făcută, iar datele nu ar trebui păstrate.

Odată ce datele au fost anonimizate complet, acestea intră din sfera de protecție a Regulamentului.

Datele pseudonimizate

GDPR încurajează pseudonimizarea datelor cu caracter personal, fiind una dintre cele mai eficiente măsuri de protecție a datelor. Aplicarea pseudonimizării datelor cu caracter personal poate reduce riscurile pentru persoanele vizate și poate ajuta operatorii și persoanele împuternicite de aceștia să își îndeplinească obligațiile de protecție a datelor.²²

Potrivit GDPR, „pseudonimizare” **înseamnă 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 informații suplimentare.**

Pseudonimizarea se poate obține, spre exemplu, prin înlocuirea unui element de identificare un cod.

Acest lucru nu înseamnă că datele vor fi separate definitive și irevocabil de numele persoanei, ci că asocierea între date și elementele de identificare nu ar trebui să fie posibilă în mod direct. Pentru persoanele care nu au cheia de decodificare, reidentificarea este dificil de realizat. În schimb, pentru persoanele care au cheia de decodificare, reidentificarea se poate face cu ușurință.

☞ *Exemplu: Propoziția „Alice Popescu, născută la 27 ianuarie 1995 are trei căței albi și iubește marea”, poate fi pseudonimizată astfel:*

„A.P. 1995 are trei căței albi și iubește marea” sau

²² Par. (28) din Preambulul Regulamentului (EU) 679/2016

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

„123 are trei căței albi și iubește marea” sau

*„T67x&*j2372A are trei căței albi și iubește marea”*

Persoanele care au acces la aceste date pseudonimizate nu au posibilitatea să o identifice pe „Alice Popescu, născută la 27 ianuarie 1995” din „123” sau „T67x&*j2372A”. Astfel, pseudonimizarea poate fi mai sigură împotriva utilizării incorecte.

Pseudonimizarea poate fi foarte utilă atunci când operatorii de date trebuie să lucreze cu aceleași persoane vizate, însă nu toți oamenii (cum ar fi angajații) trebuie să cunoască identitatea reală a persoanelor vizate. Această tehnică de pseudonimizare ar trebui inclusă în sistemele avansate de prelucrare a datelor sau a noilor tehnologii, încă din stadiul dezvoltării acestora.

2.4. Operatorul și persoana împuternicită de operator

Pe scurt

-  **Operatorul este entitatea care stabilește scopul și mijloacele prelucrării datelor.** Aici se încadrează majoritatea organizațiilor, care decid ce date să colecteze și cum să colecteze aceste date despre angajații, clienții lor etc.
-  **Persoana împuternicită este entitatea, persoana fizică sau juridică, alta decât angajatul operatorului, care prelucrează datele pe seama operatorului.** În practică, aceste persoane împuternicite sunt foarte diverse: de la firmele de HR, contabilitate, IT până la clinicile medicale care au acces la datele medicale ale angajaților.
-  **Există entități care au dublă calitate:** pe de o parte sunt operatori în legătură cu anumite date (cum ar fi datele propriilor angajați) și persoane împuternicite în legătură cu alte date (cum ar fi datele provenite de la clienții lor).
-  **Majoritatea obligațiilor impuse de GDPR cad în sarcina operatorului.** Acesta trebuie să realizeze informarea persoanei vizate, să se asigure că prelucrarea este

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

legală și că drepturile persoanei sunt onorate, să efectueze evaluări de impact etc.²³

- ✚ Totuși, persoanele împuternicite au și ele niște obligații specifice, cum ar fi să nu subîmputernicească o altă persoană fără a avea acordul prealabil al operatorului, să se asigure de securitate, să notifice operatorului în cazul unei breșe de securitate, să nu folosească datele în alte scopuri decât pentru executarea contractului cu operatorul.
- ✚ **Este recomandat ca fiecare organizație, atunci când dorește să se alinieze la prevederile GDPR, să își stabilească calitatea:** operator, persoană împuternicită sau ambele. Acest lucru este necesar pentru a ști ce obligații trebuie să respecte.
- ✚ Între operator și persoana împuternicită trebuie să existe **un contract** care să asigure protecția datelor.

Operatorul

Operatorul este definit de GDPR drept „*persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal.*”²⁴

Cu alte cuvinte, operatorul decide scopurile și mijloacele prelucrării datelor personale. Astfel, dacă organizația decide „*de ce*” și „*cum*” ar trebui prelucrate datele personale (*de exemplu* datele angajaților, clienților, abonaților, membrilor, vizitatorilor pe site), atunci ea este un operator de date. Angajații organizației vor prelucra datele pentru a îndeplini sarcinile organizației în calitate de operator.²⁵

Unul dintre cele mai importante lucruri pe care le are de făcut o organizație atunci când decide să se alinieze la GDPR, **este să determine cine este operatorul de date, deoarece**

²³ IAPP, „Data.a.d.sadasadssad”, p. 85, par. 3.

²⁴ Art. (4) pct. 7 din Regulamentul (EU) 679/2016.

²⁵ „Ce este un operator de date sau o persoană împuternicită de operator?”, material realizat de Comisia Europeană, ce poate fi accesat [aici](#).

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

lui îi revin cele mai multe obligații. Cu alte cuvinte, operatorul are sarcina responsabilității. Acesta trebuie să realizeze informarea persoanei vizate, să se asigure că prelucrarea este legală și că drepturile persoanei sunt onorate, să efectueze evaluări de impact, să se asigure că sunt respectate principiile prelucrării, să asigure securitatea și confidențialitate datelor. Majoritatea organizațiilor sunt operatori de date. Unele sunt și operatori de date și persoane împuternicite, așa cum vom arăta în cele ce urmează.

Chiar dacă nu are acces la datele personale, o organizație poate fi operator de date, așa cum este cazul magazinelor online care nu au acces la informații bancare ale clienților care realizează plata online. Aceste date sunt prelucrate de procesatorii de plăți, însă organizația care deține magazinul online va fi operatorul de date.

Pentru a stabili dacă aveți calitatea de operator, ar trebui să determinați ce control aveți cu privire la date, răspunzând la următoarele întrebări:

- a) Decide organizația ce persoane vor fi vizate de prelucrare? („**Cine?**”)
- b) Decide organizația ce categorii de date vor fi prelucrate? („**Ce?**”)
- c) Decide organizația scopul prelucrării? („**Pentru ce?**”)
- d) Decide organizația cum se va realiza prelucrarea? („**Cum?**”) – de exemplu către cine se dezvăluie datele cu caracter personal, pentru cât timp se stochează, unde se stochează etc.

Dacă majoritatea răspunsurile sunt ”**DA**”, atunci organizația este un operator de date cu caracter personal.

Pot exista și „operatori asociați”, care decid să prelucreze datele împreună pentru un scop comun. Totuși, acest scop nu trebuie să fie în totalitate comun, ci ar trebui să se suprapună măcar parțial.²⁶

☞ Exemplu: Dacă o persoană alege o vacanță de la o agenție de turism, agenție care

²⁶ IAPP, pag. 86

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

transmite mai departe datele către compania aeriană și hotel, aceștia din urmă au aceleași date, dar pentru scopuri distincte. În acest caz, fiecare entitate (agenția, compania aeriană și hotelul) sunt operatori de date. Dacă, în schimb, cele trei entități decid să își creeze un site comun și să împartă baza de date, atunci vor fi operatori asociați, chiar dacă scopurile lor nu sunt aceleași.²⁷

☞ *Exemplu: O societate oferă servicii de babysitting printr-o platformă online. În același timp, societatea are un contract cu o altă societate, care îi permite să ofere servicii cu valoare adăugată. Aceste servicii includ posibilitatea ca părinții nu doar să aleagă ce babysitter doresc, ci și să închirieze jocuri și DVD-uri pe care să le aducă babysitterul. Ambele societăți sunt implicate în organizarea tehnică a site-ului. În acest caz, cele două societăți au decis să utilizeze platforma în ambele scopuri (servicii de babysitting și închirierea de DVD-uri/jocuri) și vor partaja foarte frecvent numele clienților. Prin urmare, cele două societăți sunt operatori asociați, pentru că ele nu doar că au convenit să ofere posibilitatea unor „servicii combinate”, ci și proiectează și utilizează o platformă comună.*

Între acești operatori asociați ar trebui să existe contracte scrise cu privire la responsabilitatea fiecăruia. În principiu, fiecare operator asociat trebuie să respecte cerințele GDPR, însă pot exista situații în care unele obligații pot fi îndeplinite doar de unul dintre operatori. De exemplu, dacă doar unul dintre operatori intră în contact direct cu persoana vizată, se poate furniza o singură notă de informare către toate persoanele vizate, în numele tuturor operatorilor.²⁸

Totuși, persoana vizată își poate exercita drepturile în legătură cu oricare din acești operatori asociați.

Persoana împuternicită de operator

Persoana împuternicită este definită de GDPR drept „**persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter**

²⁷ IAPP, pag. 87

²⁸ Art. (26) din Regulamentul (EU) 679/2016.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

personal în numele operatorului”²⁹

În general, persoana împuternicită de operator va fi și operator de date în legătură cu prelucrarea pe care o efectuează în scopurile proprii, de exemplu, prelucrarea datelor angajaților sau a clienților.

Persoanele împuternicite sunt foarte diverse în actualul context economic, de la companiile de HR, contabilitate, programele de facturare, furnizorii de servicii IT, până la clinicile medicale care au acces la datele medicale ale angajaților.

☞ *Exemplu: O fabrică de bere are numeroși angajați. Aceasta semnează un contract cu o societate de administrare a statelor de plată, pentru efectuarea plății salariilor angajaților. Fabrica de bere îi spune societății de administrare a statelor de plată când trebuie plătite salariile, când un angajat părăsește fabrica sau primește o mărire de salariu și îi furnizează toate celelalte date pentru fluturașul de salariu și pentru plată. Societatea de administrare a statelor de plată furnizează sistemul informatic și stochează datele angajaților. Fabrica de bere este operatorul de date, iar societatea de administrare a statelor de plată este persoana împuternicită de operator.*

☞ *Exemplu: Un magazin online are numeroși clienți. Acesta decide să externalizeze contabilitatea și încheie un contract cu o firmă de contabilitate, căreia îi transmite periodic documente contabile, o parte din ele conținând și date personale ale clienților, precum numele, prenumele, adresa. Magazinul online va fi operatorul de date, iar firma de contabilitate va fi persoana împuternicită.*

O trăsătură comună au aceste persoane împuternicite: ele prelucrează datele provenite de la clienții lor doar pentru aceștia din urmă. Atâta timp cât respectă acest lucru și nu prelucrează datele în scopuri proprii, ele au mai puține obligații de respectat pe GDPR.

Dacă se abat de la această regulă și prelucreze datele în alte scopuri, vor fi transformați în operatori și vor avea obligația respectării celorlalte dispoziții ale GDPR, dar sunt pasibili și de a fi sancționați pentru nerespectarea obligației de a prelucra numai pentru scopul

²⁹ Art. (4) pct. 8 din Regulamentul (EU) 679/2016.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

operatorului.

☞ Exemplu: O firmă de organizări evenimente organizează, la cererea clientului său, o societate de avocatură, o conferință cu o temă juridică. Firma de organizări evenimente va colecta datele participanților la evenimente doar în scopul indicat de către societatea de avocatură, respectiv pentru organizarea conferinței. În cazul în care, peste o anumită perioadă de timp, firma de organizări organizează un eveniment similar și se gândește să îl promoveze, transmițând e-mailuri participanților la conferința juridică, iese din sfera persoanei împuternicite și se transformă în operator. În acest caz, va fi obligată să respecte toate cerințele impuse de GDPR operatorului. Cu toate acestea, o astfel de prelucrare va fi ilegală.

Relația dintre operator și persoana împuternicită de operator

Contractul

GDPR cere ca între operator și persoana împuternicită să existe un contract care: ³⁰

- stabilește **obiectul și durata prelucrării**;
- stabilește **natura și scopul prelucrării**;
- prevede **tipul de date cu caracter personal**;
- stabilește **categoriile de persoane vizate**;
- stabilește **obligațiile și drepturile operatorului**.

Respectivul contract prevede în principiu că persoana împuternicită:

- prelucrează datele personale **numai pe baza instrucțiunilor operatorului**, neputând să se abată de la ele;

³⁰ Art. 26 alin. (3) din Regulamentul (EU) 679/2016.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

- se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte **confidențialitatea**;
- adoptă toate măsurile necesare în conformitate cu articolul 32 din Regulament (pseudonimizarea și criptarea datelor cu caracter personal, confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor, restabilirea disponibilității datelor în cazul unui incident de securitate, testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării);
- **nu recrutează o altă persoană** să prelucreze datele fără acordul scris și prealabil al operatorului;
- **răspunde** pentru persoana pe care o recrutează;
- oferă asistență operatorului pentru a **răspunde cererile persoanelor vizate**;
- oferă asistență operatorului cu privire **incidentele de securitate și evaluările de impact**;
- **șterge** sau **returnează** operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare;
- permite desfășurarea **auditurilor**, inclusiv a inspecțiilor, efectuate de operator sau alt auditor mandatat și contribuie la acestea.

👉 În practică, poate fi un contract, o anexă la contract, un act adițional sau clauze incluse în contractele de prestări servicii. GDPR nu spune cine trebuie să inițieze acest contract, însă opinia majoritară este în sensul în care, ambii actori, și operatorul și persoana împuternicită au sarcina inițierii.

De regulă, operatorul este persoana care propune contractul, însă, în situația în care operatorul este o întreprindere mai mică, iar persoana împuternicită de către operator este o corporație, în practică această persoană din urmă dictează condițiile, cum este

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

cazul Google Analytics. Totuși, în aceste situații, Grupul de lucru Articolul 29 menține că standardul de responsabilitate nu trebuie coborât din cauza dezechilibrului economic.³¹

Verificarea persoanei împuternicite de către operator

GDPR spune că operatorul recurge doar la persoane împuternicite care oferă garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate care să asigure respectarea GDPR și protecția persoanei vizate.

În practică, acest lucru se poate realiza prin audituri de specialitate, în cazul prelucrărilor care prezintă riscuri (cum ar fi prelucrarea datelor sensibile sau tehnologii care pot avea o intruziune mare în viața privată) și prin chestionare, în situația unor prelucrări care nu prezintă riscuri.

👉 Important de menționat este faptul că, dacă operatorul nu recurge la persoane împuternicite de încredere, **poate fi amendat de ANSPDCP**.

2.5. Prelucrarea

Pe scurt

- 🔗 Prelucrarea datelor nu înseamnă doar colectarea sau stocarea, ci include, printre altele, consultarea sau ștergerea.
- 🔗 Regulamentul se aplică prelucrărilor automate, dar și prelucrărilor manuale, care fac parte dintr-un sistem de evidență a datelor sau sunt destinate să facă parte dintr-un astfel de sistem.
- 🔗 Regulamentul nu se aplică prelucrărilor manuale care nu fac parte dintr-un sistem de evidență a datelor sau nu sunt destinate să facă parte dintr-un astfel de sistem.

³¹ Grupul de lucru Articolul 29 (2010), Avizul 1/2010 privind conceptele de „operator” și „persoană împuternicită de către operator”, WP 169, Bruxelles, 16 februarie 2010, p. 26.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Prelucrarea este definită de Regulament³² drept orice operațiune asupra datelor personale, cum ar fi:

- colectarea;
- înregistrarea;
- organizarea;
- structurarea;
- stocarea;
- adaptarea;
- modificarea;
- extragerea;
- consultarea;
- utilizarea;
- divulgarea prin transmitere;
- diseminarea;
- punerea la dispoziție în orice alt mod;
- alinierea;
- combinarea;
- restricționarea;

³² Art. (4) pct. 2 din Regulamentul (EU) 679/2016

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

- ștergerea;
- distrugerea.

În viața de zi cu zi, se face confuzie între prelucrare și colectare sau stocare, lucru care este riscant. După cum am văzut, inclusiv operațiunea de consultare sau de ștergere este o prelucrare a datelor.

2.6. Persoana vizată

Persoana vizată este definită de Regulament drept o persoană fizică identificată sau identificabilă.

Paragraful (14) din preambulul Regulamentului prevede că *„Protecția conferită de prezentul regulament ar trebui să vizeze persoanele fizice, indiferent de cetățenia sau de locul de reședință al acestora, în ceea ce privește prelucrarea datelor cu caracter personal ale acestora. Prezentul regulament nu se aplică prelucrării datelor cu caracter personal care privesc persoane juridice și, în special, întreprinderi cu personalitate juridică, inclusiv numele și tipul de persoană juridică și datele de contact ale persoanei juridice.”*

Persoana vizată este persoana fizică la care se referă datele cu caracter personal. Persoanele decedate nu sunt persoane vizate în sensul Regulamentului³³, însă respectul datorat lor este reglementat prin art. 78-79 din Codul Civil.³⁴

Persoana vizată poate fi orice persoană fizică precum clientul, angajatul, colaboratorul, vizitatorul pe site, membrul unui ONG, abonatul la newsletter, asociatul dintr-o firmă, administratorul unei firme etc.

³³ <https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/>, accesat la data de 3.05.2018

Art. 78 din Codul Civil: „Persoanei decedate i se datorează respect cu privire la memoria sa, precum și cu privire la corpul său.”

Art. 79 din Codul Civil: „Memoria persoanei decedate este protejată în aceleași condiții ca și imaginea și reputația persoanei aflate în viață.”

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Capitolul 3. Principiile prelucrării datelor cu caracter personal

Introducere

Cuvântul „principiu” vine de la latinescul „*principium*” care semnifică începutul sau elementul fundamental.

Aceste principii sunt foarte importante și ele trebuie urmate întotdeauna pentru a respecta Regulamentul. Înainte de a lua orice decizie cu privire la o prelucrare de date, organizațiile trebuie să se asigure că respectă cumulativ toate principiile de mai jos.

GDPR³⁵ consacră **șapte principii** legate de prelucrarea datelor:

- legalitate, echitate și transparență;
- limitări legate de scop;
- reducerea la minimum a datelor;
- exactitate;
- limitări legate de stocare;
- integritate și confidențialitate;
- responsabilitate.

Primele șase principii sunt legate de activitatea de prelucrarea, așa cum vom arăta în subcapitolele următoare, iar al șaptelea, „*principiul responsabilității*” exprimă faptul că operatorul de date are obligația de a demonstra respectarea principiilor de mai sus.

3.2. Legalitate, echitate și transparență

³⁵ Art. (5) din Regulamentul (EU) 679/2016.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Pe scurt

- 📌 Datele pot fi prelucrate doar dacă există un temei juridic pentru prelucrare.
- 📌 Potrivit Regulamentului, există șase temeiuri pentru prelucrare: consimțământul, contractul, obligația legală, interesul legitim, interesul public, interesul vital.
- 📌 În absență unui temei legal, prelucrarea va fi ilegală și ea ar trebui să înceteze.

Regulamentul prevede că datele vor fi prelucrate în mod legal, echitabil și transparent față de persoana vizată („legalitate, echitate și transparență”).³⁶

Pentru a înțelege acest principiu al „legalității, echității și transparenței”, vom analiza separat cei trei piloni: legalitatea, echitatea și transparența.

Legalitatea

Legalitatea înseamnă că **datele vor fi prelucrate doar dacă există un temei juridic pentru prelucrare**. Potrivit Regulamentului, există șase temeiuri pentru prelucrare, care vor fi analizate distinct în capitolul următor:

- consimțământul;
- contractul;
- obligația legală;
- interesul legitim;
- interesul public;
- interesul vital.

În absență unui temei legal, prelucrarea va fi ilegală și ea ar trebui să înceteze. Se poate

³⁶ Art. (5) alin. (1) lit. a din Regulamentul (EU) 679/2016.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la
<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

merge simultan pe mai multe temeuri, însă alegerea acestora trebuie să se facă de la început cu atenție, întrucât migrarea ulterioară către alte temeuri nu este o practică tolerată de Regulament.

Pentru alegerea corectă a temeiului se recomandă consultarea juriștilor. Temeiurile legale ar trebui documentate pentru a putea demonstra conformitatea. Acest lucru se realizează, de regulă, prin întocmirea evidenței activităților de prelucrare.

Echitatea

Prelucrarea datelor nu trebuie să fie doar legală, cât și **corectă față de persoana vizată**. Echitatea înseamnă în principiu că acestea ar trebui să știe că datele lor sunt prelucrate și modul în care sunt prelucrate, pentru a avea toate informațiile necesare pentru a fi de acord cu prelucrarea și pentru a le permite exercitarea drepturilor. În unele cazuri, indiferent de acordul persoanei, prelucrarea este considerată echitabilă, deoarece este cerută de lege.³⁷

☞ *Exemplu: O afacere online va colecta numele, prenumele și adresa unei persoane fizice pentru emiterea unei facturi fiscale, elemente obligatorii cerute de Codul fiscal. În acest caz, prelucrarea este echitabilă, indiferent dacă persoana este de acord sau nu. Însă trebuie să ținem minte că CNP-ul nu este obligatoriu pentru emiterea facturii fiscale.*

☞ *Exemplu: O aplicație pentru livrare de catering va analiza datele personale ale clienților, în special istoricul comenzilor și al preferințelor acestora culinare (dacă de exemplu comanzi constant ciorba de burtă la prânz, când va fi în meniu la promoție vei primi o alertă). Pentru asta, aplicația folosește module de tip cookie sau alte tehnologii similare, pentru a vedea care din clienți/consumatori sunt mai predispuși să cumpere atunci când sunt notificați. Cei care fac comenzi în mod frecvent, în special care-și folosesc telefonul mobil pentru a comanda, sunt mai predispuși decât cei care comandă o dată de pe site și eventual mai deschid un newsletter, pentru că avem prea puține date despre ei. Dacă aplicația este făcută în așa fel încât să își dea seama automat ce produse/oferte să*

³⁷ <https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/>, accesat la data de 3.05.2017.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

furnizeze clienților pe baza preferințelor acestora și să afișeze, de exemplu, prețuri mai mari clienților fideli în detrimentul altora, pe ideea că aceștia comandă în mod constant și nu-și dau seama de modificarea prețurilor, o asemenea prelucrare poate fi considerată neloială.

Transparența

Deși transparența nu este definită în GDPR, totuși Paragraful (39) din Preambul este informativ cu privire la principiul transparenței: „*Ar trebui să fie transparent pentru persoanele fizice că sunt colectate, utilizate, consultate sau prelucrate în alt mod datele cu caracter personal care le privesc și în ce măsură datele cu caracter personal sunt sau vor fi prelucrate. Principiul transparenței prevede că orice informații și comunicări referitoare la prelucrarea respectivelor date cu caracter personal sunt ușor accesibile și ușor de înțeles și că se utilizează un limbaj simplu și clar. Acest principiu se referă în special la informarea persoanelor vizate privind identitatea operatorului și scopurile prelucrării, precum și la oferirea de informații suplimentare, pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoanele fizice vizate și dreptul acestora de a li se confirma și comunica datele cu caracter personal care le privesc care sunt prelucrate.*”

Art. 12 din GDPR prevede că operatorul trebuie să realizeze informarea persoanei vizate astfel:

- într-o formă concisă, transparentă, inteligibilă și ușor accesibilă;
- utilizând un limbaj clar și simplu;
- în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic;
- la solicitarea persoanei vizate, informațiile pot fi prezentate oral;
- în mod gratuit.³⁸

³⁸ <https://legalup.ro/informarea-persoanei-vizate/>, accesat la data de 3.05.2018.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

GDPR precizează că informarea persoanei ar trebui să răspundă la următoarele întrebări:

- Cine prelucrează?
- Ce tipuri de date prelucrează?
- Cui sunt transmise datele? În ce scopuri?
- Pe ce perioadă sunt stocate?³⁹

Mai multe despre informarea persoanei vizate vom discuta în capitolul următor.

Obligația de a informa așa cum prevede Regulamentul se va aplica și pentru prelucrările începute anterior 25 mai 2018.

3.3. Limitări legate de scop

Pe scurt

- ✚ Operatorul trebuie să aibă un scop clar înainte de a prelucra;
- ✚ Prelucrarea în scopuri care nu sunt clare nu este tolerată de Regulament;
- ✚ Dacă organizația transferă date către terți este nevoie de un temei suplimentar;

Datele personale trebuie colectate în scopuri determinate, explicite și legitime și nu trebuie prelucrate ulterior într-un mod incompatibil cu aceste scopuri.⁴⁰

Prelucrarea ulterioară exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice este **permisă** de Regulament.

Cu alte cuvinte, dacă organizația dorește să prelucreze datele în alt scop decât cel inițial trebuie, în primă fază, să verifice dacă noul scop are legătură cu scopul inițial. Dacă există

³⁹ Art. (13) și (14) din Regulamentul (EU) 679/2016.

⁴⁰ Art. (5) alin. (1) lit. b din Regulamentul (EU) 679/2016

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

o legătură între cele două scopuri, datele pot fi prelucrate. Dacă nu există o legătură, trebuie să se ia în calcul un nou temei juridic, iar în măsura în care acesta nu există, prelucrarea va înceta.

Pentru a se determina dacă cele două scopuri sunt compatibile, se vor lua în calcul, printre altele

- orice legătură între aceste scopuri și scopul prelucrării ulterioare;
- contextul în care au fost colectate datele cu caracter personal, în special dacă persoana vizată se poate aștepta în mod rezonabil la o prelucrare în alt scop;
- natura datelor personale;
- consecințele prelucrării ulterioare asupra persoanelor vizate;
- măsurile tehnice și organizatorice;⁴¹

☞ *Exemplu #1: Un site de comerț electronic prelucrează datele clienților pentru a oferi sugestii personalizate cu privire la produse similare de care clienții ar putea fi interesați. Prelucrarea ulterioară a datelor personale pentru a identifica erorile tehnice ale site-ului va fi considerată compatibilă deoarece îmbunătățirea performanței site-ului este compatibilă cu scopul inițial.*

☞ *Exemplu #2: O aplicație de dating online prelucrează datele utilizatorilor privitoare la sex și locație pentru a-i „cupla”. Transmiterea listei utilizatorilor către o firmă de organizări evenimente pentru a permite acestora să găsească participanți la un eveniment cu tema „Ești singur? Găsește-ți pereche pe ritm de salsa!” va fi considerată incompatibilă cu scopul inițial pentru care au fost colectate datele cu caracter personal.*

3.4. Reducerea la minimum a datelor

⁴¹ Paragraful (50) din Preambulul Regulamentului (EU) 679/2016

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Regulamentul prevede că datele trebuie să fie „adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate”⁴²

Acest principiu înseamnă că operatorul nu ar trebui să prelucreze mai multe date decât sunt necesare pentru îndeplinirea scopurilor, ci doar datele de care au nevoie în activitatea lor. O abordare de genul „păstrăm totul” nu este o practică permisă de GDPR. Datele care nu sunt necesare activității operatorului ar trebui distruse sau transformate în date anonime și folosite în scopuri statistice, istorice, de cercetare.

☞ Exemplu: O aplicație de editare foto condiționează accesul de furnizarea datelor de localizare. Deoarece aceste date nu sunt necesare pentru funcționarea aplicației, această practică nu este conformă Regulamentului.

3.5. Exactitate

Un operator care stochează date personale nu va folosi aceste date fără a lua măsuri pentru a se asigura, în mod sigur, că datele sunt exacte și actualizate.

3.6. Limitări legate de stocare

Pe scurt

-  Datele personale nu pot fi păstrate mai mult decât este necesar pentru îndeplinirea scopurilor;
-  Datele anonimizate pot fi păstrate pe termen nelimitat;
-  Se vor stabili perioade de stocare pentru fiecare categorie de date;
-  Se vor implementa măsuri pentru ștergerea, distrugerea datelor și, dacă este cazul, anonimizarea lor.

Regulamentul prevede că datele vor fi păstrate într-o formă care permite identificarea

⁴² Art. (5) alin. (1) lit. c din Regulamentul (EU) 679/2016.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele.

Cu toate acestea, 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 științifică sau istorică ori în scopuri statistice.⁴³

Cu alte cuvinte, **datele nu trebuie prelucrate mai mult decât este necesar**. După împlinirea acestei perioade, datele vor fi distruse sau șterse complet din sisteme sau transformate în date anonime.

În practică, acest lucru se realizează prin implementarea unei *Politici de retenție a datelor*, unde vor fi precizate termenele – limită pentru prelucrarea diferitelor categorii de date și prin implementarea unor soluții pentru ștergerea definitivă a datelor.

Totuși, există situații în care legea ne obligă să stocăm datele pe o anumită perioadă, cum este cazul contractelor de muncă, care se păstrează 75 de ani sau a statelor de plată, care se păstrează 50 de ani. În aceste situații, datele vor fi stocate pe perioada prevăzută de lege.

Cu privire la datele prelucrate în scopuri de marketing și considerând faptul că subiecții au dat un consimțământ valabil, datele pot fi prelucrate până când subiectul își va retrage consimțământul.

☞ Exemplu: O societate care vinde produse online prelucrează următoarele date despre clienți: numele și prenume, e-mail, telefon, adresa. Facturile care conțin date personale se vor păstra 10 ani, potrivit legii. Celelalte date ar trebui păstrate nu mai mult decât este necesar. Termenul prescripției generale de 3 ani poate fi folosit în acest caz. Cu alte cuvinte, datele personale pot fi păstrate 3 ani de la ultima comandă.

3.7. Integritate și confidențialitate

⁴³ Art. (5) alin. (1) lit.e din Regulamentul (EU) 679/2016.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Regulamentul prevede că datele vor fi 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.⁴⁴

Regulamentul nu descrie în mod clar ce măsuri tehnice sau organizatorice trebuie implementate, însă, oferă câteva puncte de plecare, cu titlu exemplificativ, următoarele:

- pseudonimizarea și criptarea datelor cu caracter personal;
- 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 și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

Aceste măsuri ar trebui să respecte, cel puțin, cerințele minime de securitate instituite prin Ordinul Avocatului Poporului nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal, așa cum vom arăta în capitolele următoare.⁴⁵

⁴⁴ Art. (5) alin. (1) lit.f din Regulamentul (EU) 679/2016.

⁴⁵ <http://www.dataprotection.ro/servlet/ViewDocument?id=861>, accesat 4.05.2018

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Capitolul 4. Legalitatea prelucrării

4.1. Introducere

Potrivit Regulamentului există șase temeiuri juridice pentru prelucrare, iar fiecare prelucrare trebuie să se bazeze pe cel puțin unul dintre temeiuri. Dacă organizația nu are un temei juridic corect identificat, prelucrarea va fi ilegală.

Temeiul juridic trebuie documentat, de regulă, prin includerea unei secțiuni în registrul prelucrărilor.

Temeiul juridic trebuie adus la cunoștința persoanelor vizate prin intermediul notelor de informare.

Regulamentul conține două seturi diferite de norme pentru prelucrarea legală a datelor: unul pentru categoriile obișnuite de date⁴⁶ și unul pentru categoriile speciale de date.⁴⁷

4.2. Legalitatea prelucrării categoriilor obișnuite de date cu caracter personal

Pe scurt

✚ Există șase temeiuri legale pentru prelucrarea datelor obișnuite;

✚ Cele șase temeiuri sunt:

- consimțământul,
- contractul,
- obligația legală,
- interesul vital,

⁴⁶ Art. (6), (7), (8) din Regulamentul (EU) 679/2016

⁴⁷ Art. (9), (10) din Regulamentul (EU) 679/2016

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

- interesul public,
 - interesul legitim;
- ✚ Dacă nu există un temei legal corect ales, prelucrarea va fi ilegală;
 - ✚ Cele șase temeiuri legale se află pe poziție de egalitate;
 - ✚ Se pot alege mai multe temeiuri pentru aceeași activitate de prelucrare, însă, migrarea ulterioară, fără o justificare corectă, nu este o practică tolerată de Regulament.
 - ✚ Prelucrarea trebuie să fie necesară. Dacă se poate atinge rezultatul altfel, prelucrarea nu va fi legală.

În continuare, vom trata separat temeiuri legale.

Consimțământul

Pe scurt

- Consimțământul, pentru a fi valabil, trebuie să îndeplinească anumite **condiții**;
- Operatorul trebuie să poată face dovada că a obținut un **consimțământ valabil**;
- Consimțământul trebuie acordat separat **pentru fiecare scop specific** al prelucrării;
- Consimțământul poate fi **retras la fel de ușor cum a fost dat**, în orice moment și în mod gratuit, dar nu neapărat prin aceeași acțiune;
- **Este nevoie de consimțământul părinților pentru prelucrarea datelor copiilor sub 16 ani.**

Consimțământul este definit de Regulament⁴⁸ drept „*orice manifestare de voință liberă,*

⁴⁸ Art. (4) pct. 11 din Regulamentul (EU) 679/2016.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

specifică, informată și 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 să fie prelucrate;”

Operatorul trebuie să poată face dovada că a obținut un consimțământ valabil.

Pentru a fi valabil, consimțământul trebuie să îndeplinească cumulativ următoarele condiții:

- să fie dat în mod liber;
- să fie specific;
- să fie informat;
- să fie lipsit de ambiguitate;

Consimțământul trebuie să fie dat în mod liber

Potrivit Grupului de Lucru Art. 29⁴⁹, consimțământul trebuie să fie o alegere reală pentru persoana vizată. Dacă persoana nu are o alegere reală, se simte obligată să își dea consimțământul sau urmează să suporte consecințe negative dacă nu își dă acordul, consimțământul nu este valabil.

☞ Exemplu: O aplicație mobilă de streaming muzical editare solicită utilizatorilor să aibă activată localizarea GPS pentru utilizarea serviciilor sale. Aplicația informează utilizatorii că va utiliza datele colectate în scopuri de publicitate comportamentală. Nici geolocalizarea și nici publicitatea comportamentală nu sunt necesare pentru furnizarea serviciului de streaming muzical. Întrucât utilizatorii nu pot utiliza aplicația fără a fi de acord cu această prelucrare, consimțământul nu poate fi considerat ca fiind acordat în

⁴⁹ Ghidul privind consimțământul elaborate de Grupul de Lucru Art. 29 <http://www.dataprotection.ro/servlet/ViewDocument?id=1442>, link accesat la data de 3.05.2018.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

În situația unui dezechilibru de putere, ca de exemplu, în relația angajator – angajat, consimțământul nu este valabil decât în cazuri excepționale. Prin urmare, recomandarea ar fi ca temeiul prelucrării datelor angajaților să nu fie consimțământul.

👉 Pentru a fi liber, consimțământul trebuie acordat separat pentru fiecare scop specific al prelucrării.

Consimțământul trebuie să fie specific

Operatorul trebuie să obțină consimțământul persoanei separat pentru fiecare activitate de prelucrare. Pentru fiecare scop, trebuie furnizate informațiile specifice cu privire la datele prelucrate. Dacă se dorește utilizarea datelor colectate în scopuri noi, trebuie obținut un nou consimțământ înainte de a prelucra datele în noile scopuri.

☞ *Exemplu: „O rețea de televiziune prin cablu colectează datele personale ale abonaților, pe baza consimțământului acestora, pentru a le prezenta sugestii personalizate pentru filme. După un timp, rețeaua TV decide că ar dori să permită terților să trimită (sau să afișeze) publicitate vizată pe baza obiceiurilor de vizionare ale abonatului. Având în vedere acest nou scop, este necesar un nou consimțământ.”*

Consimțământul trebuie să fie informat

Există **elemente obligatorii** care trebuie prezentate persoanei înainte de a i se cere consimțământul: identitatea fiecărui operator, scopul prelucrării, tipurile de date colectate, existența dreptului de retragere a consimțământului și, dacă e cazul, informații despre profilare sau decizii automate cu impact semnificativ și informații privind posibilele riscuri de transfer către state terțe UE.

Informarea trebuie să utilizeze un limbaj simplu și ușor de înțeles și trebuie să se

⁵⁰ Idem, p. 7, par. 1.

diferențieze de termenii generali. Dacă consimțământul este obținut pe hârtie, informarea trebuie să fie distinctă față de alte documente, astfel încât să se evidențieze și să atragă atenția. Utilizarea unui mod stratificat de prezentare a informației este un aspect pe care operatorii ar trebui să îl ia în calcul.

Exemplu: O companie realizează un apel de marketing către o persoană fizică. În timpul apelului, persoana este întrebată dacă dorește să fie contactată de companii terțe în scopuri de marketing. Persoana spune „da”. Apoi urmează un mesaj automat în care un robot enumeră rapid denumirea a 20 de companii care sunt incredibil de greu de înțeles într-un timp atât de scurt. **Acesta nu va fi un consimțământ informat.** În primul rând, deoarece i s-a solicitat acordul persoanei înainte ca aceasta să fie informată despre companiile terțe și în al doilea rând deoarece mesajul automat este practic imposibil de înțeles.

Consimțământul trebuie să fie lipsit de ambiguitate

Recomandarea este să se facă uz de declarații scrise, însă, întrucât acest lucru nu este întotdeauna realist se poate apela la alternative precum declarații verbale înregistrate, răspunsuri la e-mail-uri și mesaje electronice, căsuțe cu posibilitate de bifare etc.

Tăcerea, inacțiunea sau căsuțetele pre-bifate nu valorează consimțământ. Consimțământul trebuie să implice o acțiune reală, ca de exemplu o semnătură, bifarea unei căsuțe sau un răspuns clar la un e-mail.

Alte aspecte privind consimțământul

GDPR obligă operatorii să se asigure că consimțământul poate fi retras la fel de ușor cum a fost dat, în orice moment și în mod gratuit, dar nu neapărat prin aceeași acțiune. Retragera consimțământului nu trebuie să aducă prejudicii. Neîndeplinirea unui

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

mecanism de retragere duce la eșecul validității acordului. În cazul retragerii, prelucrarea care a avut loc anterior rămâne legală, însă prelucrarea ulterioară trebuie să înceteze. Un nou consimțământ valabil este necesar.

👉 Nu este permisă migrarea tacită din consimțământ către altă bază legală pentru procesare.

În privința copiilor, dacă aceștia au vârsta sub 16 ani, consimțământul trebuie dat sau autorizat de reprezentantul legal (de obicei, părintele). Statele membre pot reduce această vârstă la 13 ani. În funcție de riscul prelucrării, consimțământul părinților se va obține diferit: pentru activități cu risc scăzut se poate realiza o verificare pe e-mail, însă pentru cele cu risc mare, este nevoie de măsuri suplimentare. Odată ce copilul a ajuns la vârsta consimțământului digital (16 ani), un nou consimțământ este necesar direct de la subiect.

În situația în care consimțământul a fost obținut în conformitate cu Legea nr. 677/2001 este valabil dacă respectă condițiile stabilite de GDPR. Totuși, Grupul de Lucru Art. 29 avertizează că GDPR introduce standarde mult mai stricte care necesită revizuirea tuturor mecanismelor privind consimțământul și nu simpla actualizare a notelor de informare. Grupul avertizează în special operatorii care se bazează pe un consimțământ inactiv, cum este cazul colectării consimțământului prin utilizarea unor căsuțe pre-bifate.

👉 *Exemplu: Un blog transmite o dată pe săptămână newsletter abonaților. Consimțământul abonaților a fost luat în mod implicit, printr-o căsuță deja bifată. În acest caz, consimțământul nu este valabil, iar blogul ar trebui să colecteze un nou consimțământ care să îndeplinească standardele GDPR. Dacă persoanele nu își vor da consimțământul, prelucrarea va înceta.*

Exemplu: O companie decide să folosească baza de date a clienților pentru a trimite mesaje promoționale. Clienții nu au consimțit anterior recepționării marketing-ului, astfel încât compania trimite o scrisoare clienților prin care îi informează că urmează să le transmită informații despre promoții prin e-mail și prin poștă. În scrisoare se indică un număr de telefon unde clienții pot suna și își pot exprima poziția că nu doresc să

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

primească marketing. Inacțiunea de a răspunde nu valorează contimțământ. Prin urmare, urmând această „strategie” de obținere a consimțământului, compania nu va putea să își promoveze serviciile prin marketing direct, deoarece consimțământul nu este clar și nu implică o acțiune reală.

Contractul

Se poate utiliza acest temei atunci când există un contract valabil între operator și persoana vizată sau contractul este în fază pre-contractuală, atunci când este nevoie de prelucrarea anumitor date personal în vederea încheierii contractului.

Datele prelucrate trebuie să fie ale persoanei vizate, iar nu ale altei persoane pentru a putea utiliza acest temei juridic.

Prelucrarea trebuie să fie, de asemenea, necesară pentru încheierea sau executarea contractului.

☞ Exemplu: Dacă o persoană face o achiziție online, un operator prelucrează adresa persoanei fizice pentru a livra bunurile. Acest lucru este necesar pentru executarea contractului.

Cu toate acestea, profilarea intereselor și preferințelor unui individ pe baza elementelor achiziționate nu este necesară pentru executarea contractului, iar contractul nu poate fi folosit ca bază legală pentru această prelucrare.⁵¹

Obligația legală

Există multe situații în care organizațiile sunt obligate să prelucreze date despre alte

⁵¹<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/?template=pdf&patch=50>, link accesat 04.05.2018.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

persoane. De exemplu, angajatorii trebuie să prelucreze datele angajaților din motive de securitate socială și fiscală, iar întreprinderile trebuie să prelucreze datele clienților din motive fiscale.

Interesul vital

Acest interes, strâns legat de supraviețuirea persoanei vizate, poate constitui baza utilizării legitime a datelor privind starea de sănătate sau despre persoane dispărute, de exemplu.

Interesul public

Acest temei juridic nu este aplicabil companiilor private, de aceea nu îl vom analiza în această lucrare.

Interesul legitim

Pentru a putea recurge la interes legitim drept temei pentru prelucrare, o organizație ar trebui să efectueze un test de echilibrare pentru a determina dacă interesele sale sau a altei părți prevalează asupra drepturilor și intereselor persoanei vizate.⁵²

⁵² Opinia 06/2014 a Grupului de Lucru Art. 29.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

În continuare, vă prezentăm un scurt ghid pentru efectuarea testului de echilibrare.

PASUL 1. Calificați interesul ca fiind „legitim” sau „nelegitim”

Pentru a fi considerat legitim, un interes trebuie să îndeplinească **cumulativ** următoarele condiții:

- să fie **legal** (adică să nu încalce legislația);
- să fie **concret**;
- să **reprezinte un interes real și actual**, ca de exemplu un interes comercial (să nu fie speculativ).

👉 Dacă interesul nu îndeplinește cumulativ condițiile de mai sus, va trebui să se recurgă la alt temei juridic pentru prelucrare.

Dacă îndeplinește condițiile, adică este legitim, puteți trece la Pasul 2.

PASUL 2. Determinați dacă prelucrarea este necesară pentru atingerea interesul urmărit

Cu alte cuvinte, dacă puteți atinge același rezultat fără a prelucra datele cu caracter personal sau prin a prelucra mai puține date, nu vă puteți baza pe interesul legitim.

Dacă prelucrarea e necesară pentru obținerea rezultatului, puteți trece la Pasul 3.

PASUL 3. Efectuarea testului de echilibrare

Pentru a putea recurge la interes legitim, trebuie să efectuați un test de echilibrare din care să rezulte dacă interesele legitime prevalează asupra drepturilor și intereselor persoanei vizate.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Elemente care inclină balanța în *favoarea interesului legitim al operatorului*:

- Natura interesului (drept fundamental, interes public, interes comercial);
- Eventualul prejudiciu suferit de operator dacă prelucrarea nu are loc;
- Prelucrarea implică un grup restrâns de persoane;
- Datele nu sunt dezvăluite către terți;
- Organizația nu are o poziție dominantă pe piață;
- nu se prelucrează categorii de date speciale;
- nu există un impact semnificativ asupra drepturilor persoanei vizate;
- Persoana vizată se poate aștepta, în mod rezonabil, la existența prelucrării.

Elemente care inclină balanța în *favoarea drepturilor și intereselor persoanei vizate*:

- Eventualul prejudiciu suferit de operator dacă prelucrarea nu are loc este minor sau inexistent;
- Prelucrarea implică un grup mare de persoane;
- Datele sunt dezvăluite către terți;
- Organizația are o poziție dominantă de piață;
- Se prelucrează categorii de date speciale;
- Prelucrarea poate genera o intruziune nejustificată în viața privată a individului;
- Persoana vizată nu se poate aștepta, în mod rezonabil, la existența prelucrării.

👉 Testul de balans nu trebuie să fie abstract, indicat ar fi să se ia în calcul, în mod concret,

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

impactul pe care îl poate avea prelucrarea asupra unei anumite persoane vizate.⁵³

Exemple de situații în care se poate recurge la interes legitim: supravegherea video a angajaților la locul de muncă, colectarea datelor candidaților de către o firmă de HR, colectarea IP-ului pentru ca o organizație să se apere împotriva atacurilor cibernetice etc.

Cum se alege temeiul juridic corect pentru prelucrare?

Acest lucru depinde de scopurile specifice și de contextul prelucrării. Ar trebui să vă gândiți care bază legală se potrivește cel mai bine circumstanțelor. S-ar putea să descoperiți că se aplică mai multe temeiuri, situație în care trebuie să le identificați și să le documentați încă de la început.

Nu ar trebui adoptată o abordare unică. Niciun temei nu ar trebui privit mai important decât celelalte și nu există o ierarhie între temeiuri.

În vederea identificării temeiului corect se pot lua în calcul diverși de factori, printre care:

Care este scopul - ce dorește organizația să obțină?

Se poate atinge acest scop altfel altfel?

Aveți posibilitatea să alegeți dacă doriți sau nu să prelucrați datele?

Puteți folosi interesul legitim ca bază legală dacă doriți să păstrați controlul asupra prelucrării și să vă asumați responsabilitatea pentru a demonstra că este în concordanță cu așteptările rezonabile ale oamenilor și că nu ar avea un impact nejustificat asupra acestora. Pe de altă parte, dacă preferați să dați indivizilor controlul asupra datelor lor (inclusiv dreptul la ștergere), vă puteți baza pe consimțământ.⁵⁴

4.3. Legalitatea prelucrării categoriilor speciale de date

⁵³ Idem.

⁵⁴ <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/?template=pdf&patch=50#link2>, link accesat la 04.05.2018.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Pe scurt

- 🚦 Prelucrarea datelor sensibile este, în general, interzisă de Regulament;
- 🚦 Există totuși câteva situații în care este permisă prelucrarea datelor sensibile precum consimțământul explicit sau protejarea intereselor vitale;
- 🚦 Operatorii trebuie să asigure o securitate.

Art. 9 alin. (1) din Regulament precizează că „se interzice prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice.”

Totuși, alin. (2) al art. 9 spune că datele sensibile pot fi prelucrate doar în următoarele situații:

- a) persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepția cazului în care dreptul Uniunii sau dreptul intern prevede ca interdicția prevăzută la alineatul (1) să nu poată fi ridicată prin consimțământul persoanei vizate;

👉 O declarație scrisă semnată este cel mai bun exemplu pentru un consimțământ explicit. Alte recomandări ale Grupului de lucru Art. 29⁵⁵ sunt: un proces de verificare în doi factori a consimțământului (verificare ulterioară prin e-mail, sms, telefon pentru a se asigura că acordul este explicit), utilizarea unei semnături electronice, urcarea unui document scanat semnat, înregistrarea unei declarații verbale.

Pe lângă condițiile detaliate mai sus, operatorii au obligația de a păstra evidențele pentru a demonstra că s-a luat un consimțământ valabil și că subiectul a fost informat.

⁵⁵ <http://www.dataprotection.ro/servlet/ViewDocument?id=1470>.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

- b) prelucrarea este necesară în scopul îndeplinirii obligațiilor în domeniul ocupării forței de muncă și al securității sociale și protecției sociale, în măsura în care acest lucru este lege;
- c) prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul;
- d) 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, cu condiția ca prelucrarea să se refere numai la membrii sau la foștii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale și ca datele cu caracter personal să nu fie comunicate terților fără consimțământul persoanelor vizate;
- e) prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;
- f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare;
- g) prelucrarea este necesară din motive de interes public major;
- h) prelucrarea este necesară în 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 asistență socială, în condițiile legii;
- i) prelucrarea este necesară din motive de interes public în domeniul sănătății publice;
- j) prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice.

Prelucrarea acestor categorii de date ar putea crea riscuri mai mari pentru drepturile și

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

libertățile fundamentale ale unei persoane, cum ar fi, de exemplu, discriminarea, de aceea condițiile prelucrării sunt foarte stricte, iar măsurile de securitate implementate trebuie să fie adecvate riscurilor.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Capitolul 5. Drepturile persoanei vizate

5.1. Introducere

Pe scurt

✚ Principalele drepturile oferite persoanelor vizate de Regulament⁵⁶ sunt următoarele:

- dreptul la informare,
- dreptul de acces,
- dreptul la rectificare,
- dreptul la ștergerea datelor,
- dreptul la restricționarea prelucrării,
- dreptul la portabilitatea datelor,
- dreptul de a nu fi supus unei decizii automate cu efect semnificativ,
- dreptul la opoziție.

✚ Drepturile **nu sunt absolute și există excepții**.

✚ Răspunsul la cererea persoanei vizate se va face în termen de **o lună** de la primirea cererii, cu excepția situațiilor în care cererea este complexă sau există un număr mare de cereri, când se poate prelungi cu încă **două luni**.

✚ Dacă cererea este întemeiată, se va facilita exercitarea drepturilor. Dacă cererea nu este întemeiată, se va comunica motivul refuzului persoanei vizate și i se va comunica dreptul de a depune o plângere la ANSPDCP și dreptul de a se adresa

⁵⁶ Art. (14)- (23) din Regulamentul (EU) 679/2016

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

justiției.

- ✚ Răspunsul la cerere ar trebui să fie **gratuit**. În cazul unei cereri nefondate sau excesive, operatorul poate să perceapă o taxă rezonabilă sau să refuze să dea curs cererii.

Încă de la început, legislația europeană, dar și cea națională privind protecția datelor cu caracter personal a oferit persoanele vizate o serie de drepturi pe care și le pot exercita în raport cu organizațiile care le prelucrează datele.

În toate cazurile, societatea va decide dacă o cerere este întemeiată prin studierea Regulamentului. În unele cazuri, pentru a stabili dacă o cerere este întemeiată sau nu se vor consulta departamentul juridic al companiei sau consultanții juridici externi.

Răspunsul la cererea persoanei vizate se va face în termen de o lună de la primirea cererii, cu excepția situațiilor în care cererea este complexă sau există un număr mare de cereri, când se poate prelungi la două luni. Persoana va fi informată asupra amânării și motivului acesteia în termen de o lună de la primirea cererii. Dacă cererea este întemeiată, se va facilita exercitarea drepturilor. Dacă cererea nu este întemeiată, se va comunica motivul refuzului persoanei vizate și i se va comunica dreptul de a depune o plângere la ANSPDCP și dreptul de a se adresa justiției.

Răspunsul la cerere ar trebui să fie gratuit. În cazul unei cereri nefondate sau excesive, operatorul poate să perceapă o taxă rezonabilă sau să refuze să dea curs cererii. În situația unei investigații sau a unui litigiu, sarcina de a dovedi că cererea este nefondată sau excesivă revine operatorului.

Cum se calculează termenul de o lună?

☞ *Exemplu: O companie primește cererea pe 3 septembrie. Termenul de o lună va începe să curgă de a doua zi (4 septembrie). Acest lucru înseamnă că organizația va avea timp*

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

până pe 4 octombrie să se conformeze cererii.⁵⁷

☞ Exemplu: O companie primește cererea pe 30 martie. Termenul de o lună va începe să curgă de a doua zi (31 martie). Deoarece nu există data de 31 aprilie, înseamnă că organizația va avea timp până pe 30 aprilie să se conformeze cererii. Dacă termenul de 30 aprilie cade într-o zi nelucrătoare, compania are timp până în următoarea zi lucrătoare să răspundă.⁵⁸

5.2. Dreptul la informare

Pe scurt

- ✚ Persoanele vizate au dreptul să fie informate despre felul în care organizațiile le prelucrează datele;
- ✚ Informarea trebuie realizată, dacă datele provin de la subiect, la momentul colectării datelor;
- ✚ Datele provin din alte surse, informarea se va realiza în mult o lună de la momentul obținerii datelor;
- ✚ Informarea trebuie să fie concisă, transparentă, inteligibilă, ușor accesibilă și într-un limbaj simplu și clar;
- ✚ Informarea copiilor trebuie să se realizeze într-un limbaj pe care aceștia îl pot înțelege.⁵⁹

Art. 12 din Regulament prevede că operatorul trebuie să realizeze informarea persoanei vizate astfel:

⁵⁷<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/?template=pdf&patch=50>, link accesat 5.05.2018.

⁵⁸ Idem.

⁵⁹ <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/?template=pdf&patch=50>, link accesat la 5.05.2018.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

- într-o formă concisă, transparentă, inteligibilă și ușor accesibilă;
- utilizând un limbaj clar și simplu;
- în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic;
- la solicitarea persoanei vizate, informațiile pot fi prezentate oral;
- informarea trebuie să fie gratuită.

Forma concisă, transparentă, inteligibilă și ușor accesibilă

Grupul de Lucru Art. 29⁶⁰ recomandă ca informațiile să fie prezentate succint și să se diferențieze în mod clar de alte informații, ca de exemplu, dispozițiile contractuale.

Cerința ca informația să fie „*inteligibilă*” înseamnă că ar trebui înțeleasă de un membru mediu al publicului vizat.

Cerința „*ușor accesibilă*” înseamnă că persoana vizată nu ar trebui să caute ea însăși informațiile, ci să îi fie gata oferite de către operator. Grupul de lucru recomandă ca pentru accesarea notei de informare să nu se folosească mai mult de două clickuri și că funcția de meniu utilizată în aplicații ar trebui să includă întotdeauna o secțiune pentru protecția datelor.

☞ *Exemplu: Fiecare organizație care are un site web ar trebui să dețină o Politică de confidențialitate/Notă de informare privind protecția datelor. Un link către această Politică de confidențialitate trebuie să fie accesibil pe fiecare pagină a site-ului (de exemplu, "Confidențialitate", "Politică de confidențialitate" sau "Notă de informare privind protecția datelor").*

☞ *Exemplu: Pentru aplicații, nota de informare ar trebui, de asemenea, să fie disponibilă înainte de download. Odată ce aplicația este instalată, informațiile trebuie să fie ușor*

⁶⁰ Ghidul privind transparența al Grupului de Lucru Art. 29.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

accesibile în interiorul aplicației. O modalitate de a îndeplini această cerință este să se asigure că informațiile nu depășesc niciodată mai mult de click-uri.

Ar trebui să nu se folosească mai mult de două clickuri și funcția de meniu utilizată în aplicații ar trebui să includă întotdeauna o secțiune pentru protecția datelor.⁶¹

Limbaaj simplu și clar

Informațiile prezentate trebuie incluse într-un limbaj simplu și clar.

☞ Exemplu: Informare greșită:

„putem folosi datele tale să dezvoltăm noi servicii” (deoarece nu este clar despre ce servicii este vorba);

„putem folosi datele tale în scopuri de cercetare” (deoarece nu este clar despre ce fel de cercetare este vorba);

„putem folosi datele să îți oferim servicii personalizate” (deoarece nu este clar despre ce servicii personalizate este vorba);⁶²

☞ Exemplu: Informare corectă:

"Vom analiza istoricul de cumpărături și vom folosi detalii despre produsele pe care le-ați achiziționat anterior pentru a vă face sugestii pentru alte produse de care ați putea fi interesat" (este clar ce tipuri de date vor fi prelucrate și că datele vor fi prelucrate astfel încât reclamele personalizate să ajungă la persoana vizată)

"Vom păstra informațiile privind vizitele tale recente pe site-ul nostru și felul cum vă deplasați în diferite secțiuni ale site-ului pentru a analiza modul în care oamenii utilizează site-ul pentru a-l face mai intuitiv" (este clar ce tip de date vor fi procesate și scopul).

⁶¹ Idem, pag. 8.

⁶² Idem, pag. 9.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

În scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic

„Alte mijloace” pot include declarații/notificări de confidențialitate stratificate, ferestre pop-up, notificări 3D etc.

La solicitarea persoanei vizate, informațiile pot fi prezentate oral

În cazul în care informațiile sunt furnizate oral, operatorul ar trebui să permită persoanei vizate să asculte din nou mesajele înregistrate.

Informarea trebuie să fie gratuită

Un operator nu poate solicita o taxă pentru informarea persoanei vizate.

Notificările existente ar putea avea nevoie de actualizare. Operatorul trebuie să se asigure că notele de informare include toate informațiile prevăzute în Articolele 13 și 14 din GDPR, în caz contrar, este nevoie ca acestea să fie actualizate pentru a corespunde noilor standarde.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Ce ar trebui să conțină în mod obligatoriu nota de informare/politica de confidențialitate?

Ce informații trebuie comunicate persoanei vizate?	Datele sunt obținute direct de la persoana vizată	Datele sunt obținute din alte surse
Identitatea și datele de contact ale operatorului și, dacă este cazul, ale responsabilului cu protecția datelor	✓	✓
Scopurile și temeiurile legale ale prelucrării	✓	✓
Dacă e cazul, interesul legitim al operatorului sau al unui terț	✓	✓
Categoriile de date cu caracter personal		✓
Destinatarii sau categoriile de destinatari	✓	✓
Detalii în privința transferurilor către state din afara SEE	✓	✓
Perioada de retenție sau criteriile utilizate pentru determinarea	✓	✓

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

perioadei

Drepturile persoanei vizate

✓

✓

Dacă e cazul, existența dreptului de retragere a consimțământului

✓

✓

Dreptul de a depune o plângere la Autoritatea de supraveghere

✓

✓

Sursa de unde provin datele și dacă această sursă este una publică

✓

Dacă obligația de a divulga datele stă la baza unui contract sau a unei obligații legale și consecințele nedivulgării acestor date

✓

Existența unui proces decizional automat cu impact semnificativ asupra persoanei, inclusiv crearea de profiluri și consecințele

✓

✓

Când se vor furniza informațiilor

La momentul
colectării datelor

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

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

persoana vizată, cel târziu în momentul primei comunicări către persoana vizată 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 oară⁶³

⁶³ <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/>.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Informarea copiilor

Dacă se prelucrează date cu caracter personal ale copiilor, limbajul trebuie să fie adecvat vârstei. Grupul de Lucru Art. 29 oferă ca exemplu pentru un limbaj adresat copilului „Convenția ONU privind drepturile copilului” în limbaj pentru copii.

Modificarea notei de informare

Dacă se dorește modificarea notei de informare, această modificare ar trebui să fie într-o modalitate adecvată (de exemplu, prin e-mail) și să fie dedicată acestui subiect. Nu se recomandă informarea despre modificare împreună cu conținutul despre marketing. Ar trebui ca informarea să se realizeze cu o marjă de timp adecvată înainte de aplicarea modificării dacă implică o modificare fundamentală a naturii prelucrării sau este vorba despre o modificare care poate avea un impact semnificativ asupra persoanei.

Excepțiile de la informarea persoanei vizate

Art. 14 alin. (5) din Regulament conține excepțiile de la obligația de informare. Aceste excepții ar trebui interpretate limitativ:

- a) persoana vizată deține deja informațiile;
- b) furnizarea acestor informații se dovedește a fi imposibilă sau ar implica eforturi disproporționate, în special în cazul prelucrării în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, sub rezerva condițiilor și a garanțiilor prevăzute la articolul 89 alineatul (1), sau în măsura în care obligația menționată la alineatul (1) din prezentul articol este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective. În astfel de cazuri, operatorul ia măsuri adecvate pentru a proteja drepturile, libertățile și interesele legitime ale persoanei vizate, inclusiv punerea informațiilor la dispoziția publicului;
- c) obținerea sau divulgarea datelor este prevăzută în mod expres de dreptul Uniunii sau de dreptul intern sub incidența căruia intră operatorul și care prevede măsuri adecvate pentru a proteja interesele legitime ale persoanei vizate; sau
- d) în cazul în care datele cu caracter personal trebuie să rămână confidențiale în temeiul

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

unei obligații statutare de secret profesional reglementate de dreptul Uniunii sau de dreptul intern, inclusiv al unei obligații legale de a păstra secretul.

5.3. Dreptul de acces

Persoana vizată are dreptul să solicite organizației o confirmare că datele personale sunt prelucrate, iar în caz afirmativ, are dreptul de a obține o copie a acestor date, precum și următoarele informații:

- Scopurile prelucrării;
- Categoriile datelor cu caracter personal în cauză;
- Destinatarii sau categoriile de destinatari ai datelor, dacă există, în special orice țări terțe sau organizații internaționale;
- Durata de stocare a datelor cu caracter personal (sau criteriile utilizate pentru stabilirea acestei perioade);
- Drepturile persoanei vizate la rectificarea sau ștergerea datelor sale cu caracter personal și restricționarea sau opoziția față de prelucrare;
- Dreptul persoanei vizate de a depune o plângere la o autoritate de supraveghere;
- Informații privind sursa datelor, dacă nu provin direct de la persoana vizată;
- Dacă datele personale vor face obiectul unor decizii automate, inclusiv crearea de profiluri și, dacă da, logica acestei decizii sau profilări și eventualele consecințe implicate;
- În cazul în care datele sunt transferate unei țări terțe sau unei organizații internaționale, informații privind garanțiile care se aplică;

În cele mai multe cazuri, va trebui să dam acces persoanei la date, cu excepția situației

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

când cererea este vădit nefondată sau excesivă.

Acest drept nu este absolut: exercitarea acestuia nu ar trebui să afecteze drepturile și libertățile altora, cum ar fi secretele comerciale sau proprietatea intelectuală.

☞ Exemplu: O companie care deține o sală de fitness permite membrilor să își facă rezervări online prin intermediul unei aplicații. Membrul poate solicita companiei să îi furnizeze toate informațiile stocate. În acest caz, compania va furniza toate informațiile, cum ar fi: data la care membrul a început să utilizeze serviciile, clasele la care a participat, dacă a întârziat vreodată la clase și eventualele penalități care s-au aplicat.

5.4. Dreptul la rectificare

În cazul în care datele cu caracter personal sunt inexacte, persoana vizată are dreptul să solicite corectarea și completarea datelor personale incomplete pe baza informațiilor pe care le furnizează.

Dacă este necesar, va lua măsuri suplimentare pentru a verifica dacă informațiile furnizate de persoană sunt corecte înainte de a opera modificarea.

☞ Exemplu: O persoană utilizează o platformă de e-learning pentru urmarea unor cursuri online. Contul de e-mail al persoanei a fost spart și nu a reușit să îl recupereze. Persoana și-a creat nou cont de e-mail, însă nu mai poate utiliza platforma de e-learning. Prin urmare, se poate adresa companiei pentru actualizarea e-mailului, iar aceasta, după ce verifică identitatea persoanei, îi va rectifica adresa de e-mail și îi va permite accesul în cont.

5.5. Dreptul la ștergerea datelor

Persoana vizată are dreptul să solicite operatorului să șteargă fără întârziere datele cu caracter personal care o privesc în următoarele cazuri:

- datele cu caracter personal **nu mai sunt necesare** pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

- persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea și nu există niciun alt temei juridic pentru prelucrare;
- persoana vizată 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 legii;
- datele cu caracter personal au fost colectate în legătură cu oferirea de servicii online copiilor.

Operatorul va trebui să ia o decizie cu privire la o astfel de solicitare. Ștergerea datelor nu se va realiza dacă:

- datele sunt necesare pentru exercitarea dreptului la liberă exprimare și informare;
- datele sunt necesare pentru îndeplinirea unei obligații legale;
- din motive de interes public în domeniul sănătății publice;
- în scopuri de arhivare în interes public;
- pentru constatarea, exercitarea sau apărarea unui drept în instanță.

☞ Exemplu: O persoană decide să părăsească un site de rețele sociale. Are dreptul de a-i cere operatorului să șteargă datele cu caracter personal care îi aparțin, iar operatorul va trebui să se conformeze.

☞ Exemplu: O persoană decide să părăsească un site de rețele sociale. Pe acest site, persoana a cumpărat servicii de publicitate. Persoana înaintează o cerere de ștergere a datelor. Compania realizează că poate șterge datele, însă legea o obligă să păstreze timp de 10 ani facturile emise către persoană. Prin urmare, va șterge doar o parte din date,

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

păstrându-le pe cele care trebuie păstrate potrivit legii.

☞ Exemplu: O publicație online a publicat, la cererea unor elevi nemulțumiți, un articol defăimător despre o profesoară. Acesta înaintează o cerere de ștergere a datelor, iar publicația este obligată să o șteargă, deoarece informația nu este de interes public.

5.6. Dreptul la restricționarea prelucrării

Persoana vizată își poate exercita dreptul la restricționarea prelucrării în următoarele situații:

- persoana vizată contestă exactitatea datelor, pentru o perioadă care îi 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; sau
- persoana vizată s-a opus prelucrării pentru intervalul de timp în care se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate.

Organizația, în situația în care primește o cerere de restricționare, va trebui să verifice dacă cererea se încadrează într-unul din cazurile de mai sus. Pentru a se lua o decizie potrivită, este recomandat să se apeleze la Responsabilul cu protecția datelor, ori, în situația în care organizația nu a desemnat un responsabil, la departamentul juridic sau consilierii legali ai firmei (de exemplu, avocații).

În cazul în care se vor restricționa datele, acestea vor rămâne stocate, dar nu pot fi prelucrate fără consimțământul persoanei. Ele vor putea fi prelucrate pentru constatarea, exercitarea sau apărarea unui drept în instanță sau pentru protecția drepturilor unei alte

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

persoane fizice sau juridice sau din motive de interes public important al Uniunii sau al unui stat membru.

În toate cazurile, persoana vizată care a obținut restricționarea prelucrării este informată de către operator înainte de ridicarea restricției de prelucrare.

☞ Exemplu: O persoană a cumpărat două bilete la un concert al formației preferate prin intermediul unei societăți de vânzări de bilete online. După aceea este bombardat(ă) cu reclame la concerte și evenimente care nu o interesează. Persoana informează compania de vânzări de bilete că nu mai dorește să primească materialul publicitar. Compania ar trebui să înceteze a mai prelucra datele cu caracter personal pentru marketing direct și, în scurt timp, persoana ar trebui să nu mai primească e-mailuri de la aceasta. Societatea nu ar trebui să perceapă nicio taxă în acest scop.⁶⁴

5.7. Dreptul la portabilitatea datelor

Persoana vizată are dreptul să solicite ca datele personale să fie furnizate într-un format "*structurat, utilizat în mod obișnuit și care poate fi citit de mașină*" și să transfere datele respective unei alte părți, de exemplu unui alt furnizor de servicii. Aceasta se aplică datelor cu caracter personal pentru care prelucrarea se bazează pe consimțământul persoanei vizate, pe temeiul legal al contractului sau în situația în care prelucrarea este efectuată prin mijloace automate.

Acolo unde este posibil din punct de vedere tehnic, persoana vizată poate, de asemenea, solicita ca datele personale să fie transferate direct de la un operator la altul.

☞ Exemplu: Un membru al unei rețele sociale online decide că o nouă rețea socială concurentă este mai potrivită pentru obiectivele și grupa lui de vârstă. Acesta poate solicita rețelei sociale online pe care o utilizează în prezent să transfere datele cu caracter

⁶⁴ https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-ask-company-organisation-stop-processing-my-personal-data_ro, link accesat la 5.5.2018.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

personal, inclusiv fotografiile, la noua rețea socială.⁶⁵

☞ Exemplu: O persoană a găsit o aplicație online de facturare care are prețuri mai mici. Persoana poate cere furnizorului actual să transmită datele direct către noul furnizor, dacă acest lucru este fezabil din punct de vedere tehnic. În orice caz, compania trebuie să îi returneze datele clientului într-un format utilizat în mod curent și prelucrabil automat, pentru ca acestea să poată fi utilizate pe alte sisteme.⁶⁶

5.8. Dreptul la opoziție

Persoana vizată are dreptul de a se **opune prelucrării** care se bazează pe interesul legitim al operatorului sau al unei terțe părți sau interesul public.

Odată ce obiecția a fost făcută, organizația trebuie să justifice motivele pe care se bazează prelucrarea și să suspende prelucrarea până când decizia a fost luată. Organizația nu va mai prelucra datele cu caracter personal, cu excepția cazului în care demonstrează că are motive legitime și imperioase 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.

În cazul în care datele cu caracter personal sunt utilizate pentru marketingul direct, organizația va înceta prelucrarea.

5.9. Procesul decizional individual automatizat, inclusiv crearea de profiluri

Persoana vizată are dreptul să nu facă obiectul unei decizii automate, inclusiv crearea de profiluri în cazul în care decizia are un efect semnificativ sau juridic asupra acesteia. Persoana vizată are, de asemenea, dreptul de a-și exprima punctul de vedere, de a solicita intervenție umană și de a contesta decizia.

⁶⁵ https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-ask-company-organisation-send-me-my-personal-data-so-i-can-use-it-somewhere-else_ro, link accesat 5.5.2018

⁶⁶ <http://blog.avocatoo.ro/gdpr-si-dreptul-la-portabilitatea-datelor-cu-caracter-personal/>, link accesat 5.5.2018

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Există excepții de la acest drept, care sunt în cazul în care decizia:

1. Este **necesară pentru încheierea sau executarea contract**;
2. Este **autorizată prin lege națională sau europeană**;
3. Se bazează pe **consimțământul explicit** al persoanei vizate;

În situațiile de la punctele (1) și (2), organizația va pune în aplicare măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate, cel puțin dreptul acestuia de a obține intervenție umană din partea operatorului, de a-și exprima punctul de vedere și de a contesta decizia.

Pentru a evalua temeinicia unei astfel de cereri, organizația va trebui să decidă dacă excepțiile de mai sus se vor aplica situației. Pentru a se lua o decizie potrivită, este recomandat să se apeleze la responsabilul cu protecția datelor, ori, în situația în care organizația nu a desemnat un responsabil, la departamentul juridic sau consilierii legali ai firmei.

Unele organizații, cum sunt băncile, birourile administrației financiare și spitalele, utilizează algoritmi pentru a lua decizii în privința persoanelor fizice, folosind date cu caracter personal. Pentru aceste organizații este eficient, dar nu întotdeauna transparent, iar aceste decizii pot afecta din punct de vedere juridic sau pot avea un alt impact semnificativ asupra vieții persoanelor.

În asemenea cazuri, organizațiile trebuie:

- să spună dacă decizia lor este automatizată;
- să dea dreptul de a solicita analizarea deciziei automatizate de către o persoană;
- să permită persoanelor să conteste decizia automatizată.

Deciziile bazate pe prelucrarea automată sunt permise în anumite situații, de exemplu, atunci când o anumită lege permite acest lucru.

☞ Exemplu: O persoană solicită un împrumut de la o bancă online. I se cere să introducă

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

datele, iar algoritmul băncii îi spune dacă va acorda împrumutul și prezintă rata dobânzii propuse. Persoana poate: să își exprime opinia, să conteste decizia și să solicite implicarea unei persoane în proces care să verifice decizia algoritmului. ⁶⁷

⁶⁷ <https://legalup.ro/vrei-un-imprumut-dar-decizia-o-ia-masina-gdpr-solutia/> link accesat 5.5.2018

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Capitolul 6. Incidentele de securitate

Pe scurt

- ✚ Incidentele pot apărea sub diverse forme: de la un print screen neautorizat al unui ecran unde apar date personale, uitarea unui laptop în taxi până la atacuri cibernetice;
- ✚ Orice incident de securitate trebuie notificat, cu excepția cazului în care incidentul nu prezintă riscuri pentru persoana vizată;
- ✚ Dacă incidentul prezintă riscuri ridicate pentru persoanele vizate, acesta trebuie notificat atât Autorității de Supraveghere, cât și persoanelor vizate.
- ✚ GDPR impune ca notificarea să aibă loc „*fără întârzieri nejustificate*” dacă încălcarea este susceptibilă să genereze „*un risc ridicat pentru drepturile și libertățile persoanelor fizice*”;
- ✚ Notificarea se va face în termen de **72 de ore de la descoperirea incidentului**;
- ✚ În cazul în care notificarea nu poate fi făcută în 72 ore trebuie să se motiveze întârzierea.
- ✚ Notificarea se va realiza la adresa de e-mail brese@dataprotection.ro, cu excepția cazului în care ANSPDCP va indica o altă modalitate pentru transmiterea notificării.
- ✚ Notificarea persoanelor vizate **nu este obligatorie** în situația în care ar necesita „eforturi disproporționate” din partea operatorului.

O cerință a Regulamentului UE 679/2016 (GDPR) este ca incidentele de securitate cu privire datele cu caracter personal care pot avea un risc pentru drepturile și libertățile persoanelor vizate trebuie raportate Autorității de Supraveghere (ANSPDCP) fără întârzieri nejustificate, în termen de 72 de ore de la conștientizarea acestora. În cazul în care notificarea nu poate fi făcută în 72 ore trebuie să se motiveze întârzierea.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

În cazul în care un incident afectează datele cu caracter personal, trebuie luată o decizie dacă incidentul poate conduce la un risc asupra drepturilor și libertăților persoanei fizice vizate. GDPR impune ca notificarea să aibă loc „fără întârzieri nejustificate” dacă încălcarea este susceptibilă să genereze „un risc ridicat pentru drepturile și libertățile persoanelor fizice”.

Natura exactă a unui incident și impactul acestuia nu pot fi prezise cu niciun grad de certitudine și, prin urmare, este important să se utilizeze o atenție deosebită atunci când se decide ce acțiuni vor fi întreprinse.

Procedura de notificare a incidentelor de securitate

Odată ce s-a aflat că a avut loc un incident de securitate asupra datelor cu caracter personal, există două entități cu privire la care trebuie luată decizia dacă vor fi notificate sau nu. Acestea sunt:

1. Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP);
2. Persoanele vizate afectate.

Nu întotdeauna un incident de securitate trebuie notificat, ci doar în situația în care incidentul prezintă un risc pentru „drepturile și libertățile persoanelor fizice” (articolul 33 din GDPR).

Următoarele secțiuni descriu modul în care trebuie luată această decizie și ce trebuie făcut în cazul în care este necesară notificarea.

Organizația va decide dacă va notifica ANSPDCP sau nu

GDPR prevede că o încălcare a securității datelor cu caracter personal va fi notificată Autorității de Supraveghere „cu excepția cazului în care este puțin probabil ca încălcarea securității datelor cu caracter personal să ducă la un risc pentru drepturile și libertățile persoanelor fizice” (articolul 33 din GDPR). Acest lucru presupune ca organizația să evalueze nivelul riscului înainte de a decide dacă trebuie sau nu să notifice.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Factorii care trebuie luați în considerare ca parte a acestei evaluări a riscurilor ar trebui să includă:

- Datele personale au fost criptate;
- Dacă au fost criptate, cât de înalt a fost nivelul de criptare;
- În ce măsură datele au fost pseudonimizate;
- Categoriile de date afectate (de exemplu nume, adresă, detalii bancare, date biometrice) și dacă au fost afectate categorii speciale de date;
- Volumul de date afectate;
- Numărul persoanelor vizate afectate;
- Natura incidentului (furt, pierderea unui laptop, distrugerea accidentală);
- Orice alți factori care sunt considerați relevanți.

Persoanele implicate în această evaluare a riscurilor ar trebui să includă persoane din următoarele departamente: Management, IT, Juridic, Responsabilul cu Protecția Datelor (DPO).

Metoda de evaluare a riscurilor, raționamentul și concluziile sale ar trebui să fie pe deplin documentate și semnate de conducere. Rezultatul evaluării riscurilor ar trebui să includă una dintre următoarele concluzii:

1. Încălcarea datelor cu caracter personal nu necesită notificare;
2. Încălcarea datelor cu caracter personal necesită doar notificarea către Autoritatea de Supraveghere (ANSPDCP);
3. Încălcarea datelor cu caracter personal necesită notificarea atât Autorității de Supraveghere (ANSPDCP), cât și persoanelor vizate.

Aceste concluzii pot fi supuse schimbării ca urmare a feedbackul-ului Autorității de Supraveghere (ANSPDCP) sau ulterior, ca urmare a descoperirii altor informații suplimentare din care rezultă că impactul este grav și incidentul prezintă un risc asupra persoanelor fizice.

Cum se notifică Autoritatea de Supraveghere

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

În cazul în care se decide să se realizeze notificarea către Autoritatea de Supraveghere, o cerință a Regulamentului UE 679/2016 (GDPR) este ca incidentele de securitate cu privire datele cu caracter personal care pot avea un risc pentru drepturile și libertățile persoanelor vizate trebuie raportate Autorității de Supraveghere (ANSPDCP) fără întârzieri nejustificate, în termen de 72 de ore de la conștientizarea acestora. În cazul în care notificarea nu poate fi făcută în 72 ore trebuie să se motiveze întârzierea.

Notificarea se va realiza la adresa de e-mail brese@dataprotection.ro, cu excepția cazului în care ANSPDCP va indica o altă modalitate pentru transmiterea notificării.

Notificarea va cuprinde, cel puțin, următoarele:

- (a) caracterul încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;
- (b) numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
- (c) consecințele probabile ale încălcării securității datelor cu caracter personal;
- (d) măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

Există un formular de notificare online, disponibil la adresa <http://www.dataprotection.ro/servlet/ViewDocument?id=1100>, care poate fi folosit pentru notificare.

Organizația va decide dacă va notifica persoanele vizate sau nu

GDPR afirmă „în cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.”

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Prin urmare, notificarea ANSPDCP se va face atunci când incidentul de securitate prezintă un risc, iar notificarea persoanelor vizate și ANSPDCP se va realiza atunci când incidentul prezintă un risc ridicat.

Factorii care trebuie luați în considerare ca parte a acestei evaluări a riscurilor ar trebui să includă:

- Datele personale au fost criptate;
- Dacă au fost criptate, cât de înalt a fost nivelul de criptare;
- În ce măsură datele au fost pseudonimizate;
- Categoriile de date afectate (de exemplu nume, adresă, detalii bancare, date biometrice) și dacă au fost afectate categorii speciale de date;
- Volumul de date afectate;
- Numărul persoanelor vizate afectate;
- Natura incidentului (furt, pierderea unui laptop, distrugerea accidentală);
- Orice alți factori care sunt considerați relevanți.

Persoanele implicate în această evaluare a riscurilor ar trebui să includă persoane din următoarele departamente: Management, IT, Juridic, Responsabilul cu Protecția Datelor (DPO).

Aceste concluzii pot fi supuse schimbării bazate pe feedbackul Autorității de Supraveghere (ANSPDCP) sau ulterior, ca urmare a descoperirii a altor informații suplimentare din care rezultă că impactul este grav și incidentul prezintă un risc ridicat asupra persoanelor fizice.

Notificarea persoanelor vizate nu este obligatorie în situația în care ar necesita „eforturi disproporționate” din partea operatorului.

Cum se notifică persoanele vizate

Odată ce s-a decis că trebuie notificate persoanele vizate GDPR cere ca acest lucru să se facă fără întârzieri nejustificate.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Comunicarea către persoanele vizate afectate va descrie în limbaj simplu și clar natura încălcării securității datelor cu caracter personal (articolul 34 din GDPR) și trebuie să cuprindă și:

(b) numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;

(c) consecințele probabile ale încălcării securității datelor cu caracter personal;

(d) măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

În plus față de punctele solicitate de GDPR, ar putea fi oportun să se ofere ajutor persoanei vizate cu privire la acțiunile pe care acestea le pot lua pentru a reduce riscurile asociate cu încălcarea securității datelor cu caracter personal.

În majoritatea cazurilor, este oportună notificarea persoanelor vizate afectate prin poștă, e-mail sau ambele, pentru a se asigura că mesajul a fost primit și că au posibilitatea de a lua orice acțiune necesară.

☞ Exemplu: Un angajat al unei aplicații medicale decide să copieze datele clienților pe un CD și le publică online. Compania află câteva zile mai târziu. Din momentul în care află, compania are la dispoziție 72 de ore pentru a informa autoritatea de supraveghere și, deoarece datele cu caracter personal sunt date sensibile (date privitoare la sănătate), au fost publicate online și nu au fost luate măsuri de securitate, precum pseudonimizarea sau criptarea, compania ar trebui să informeze și persoanele vizate.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Capitolul 7. Securitatea prelucrării

Pe scurt

- ✚ Operatorul și persoana împuternicită ar trebui să implementeze măsuri tehnice și organizatorice adecvate pentru a asigura securitatea datelor.
- ✚ Măsurile de securitate implementate ar trebui să fie proporționale cu riscul asupra drepturilor persoanelor, costurile implementării și stadiul actual al dezvoltării.
- ✚ Organizațiile ar trebui să respecte și cerințele minime de securitate instituite de Ordinul Avocatului Poporului nr. 52/2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.

Art. 32 din Regulament prevede faptul că operatorul și persoana împuternicită ar trebui să implementeze măsuri tehnice și organizatorice adecvate pentru a asigura securitatea datelor.

Măsurile de securitate implementate ar trebui să fie proporționale cu riscul asupra drepturilor persoanelor, costurile implementării și stadiul actual al dezvoltării.

Regulamentul nu definește sintagma „măsuri tehnice și organizatorice”, ci lasă la latitudinea operatorului și a persoanei împuternicite implementarea unor măsuri adecvate, însă oferă, cu titlu de exemplu, câteva direcții:

- (a) pseudonimizarea și criptarea datelor cu caracter personal;
- (b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continuă ale sistemelor și serviciilor de prelucrare;
- (c) capacitatea de a restabili disponibilitatea datelor cu caracter personal și 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 și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Pe lângă acestea, organizațiile ar trebui să respecte și cerințele minime de securitate instituite de Ordinul Avocatului Poporului nr. 52/2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.⁶⁸

Cerințele minime de securitate a prelucrărilor de date cu caracter personal instituite de Ordinul Avocatului Poporului nr. 52/2002 acoperă următoarele aspecte:

Identificarea și autentificarea utilizatorului

Prin utilizator se înțelege orice persoană care acționează sub autoritatea operatorului, a persoanei împuternicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal.

Utilizatorii, pentru a căpăta acces la o bază de date cu caracter personal, trebuie să se identifice. Identificarea se poate face prin mai multe metode, cum ar fi: introducerea codului de identificare de la tastatură (un șir de caractere), folosirea unei cartele cu cod de bare, folosirea unei cartele inteligente (smart card) sau a unei cartele magnetice.

Fiecare utilizator are propriul său cod de identificare. Niciodată mai mulți utilizatori nu trebuie să aibă același cod de identificare.

Codurile de identificare (sau conturi de utilizator) nefolosite o perioadă mai îndelungată trebuie dezactivate și distruse după un control prealabil intern al operatorului. Perioada după care codurile trebuie dezactivate și distruse se stabilește de operator.

Orice cont de utilizator este însoțit de o modalitate de autentificare. Autentificarea poate fi făcută prin introducerea unei parole sau prin mijloace biometrice: amprenta dactiloscopică, amprenta vocală, angiografia retiniană etc.

Parolele sunt șiruri de caractere. Cu cât șirul de caractere este mai lung, cu atât parola este mai greu de aflat. La introducerea parolelor acestea nu trebuie să fie afișate în clar pe monitor. Parolele trebuie schimbate periodic în funcție de politicile de securitate ale entității (operator sau persoană împuternicită). Schimbarea periodică a parolelor se face

⁶⁸ <http://www.dataprotection.ro/servlet/ViewDocument?id=861>, link accesat 05.05.2018

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

numai de către utilizatori autorizați de operator.

Operatorul trebuie să solicite realizarea unui sistem informațional care să refuze automat accesul unui utilizator după 5 introduceri greșite ale parolei.

Orice utilizator care primește un cod de identificare și un mijloc de autentificare trebuie să păstreze confidențialitatea acestora și să răspundă în acest sens în fața operatorului.

Fiecare entitate va stabili o procedură proprie de administrare și gestionare a conturilor de utilizator.

Operatorii autorizează anumiți utilizatori pentru a revoca sau a suspenda un cod de identificare și autentificare, dacă utilizatorul acestora și-a dat demisia ori a fost concediat, și-a încheiat contractul, a fost transferat la alt serviciu și noile sarcini nu îi solicită accesul la date cu caracter personal, a abuzat de codurile permise sau dacă va absenta o perioadă îndelungată stabilită de entitate.

Accesul utilizatorilor la bazele de date cu caracter personal efectuate manual se va face pe baza unei liste aprobate de conducerea entității.

Tipul de acces

Utilizatorii trebuie să acceseze numai datele cu caracter personal necesare pentru îndeplinirea atribuțiilor lor de serviciu. Pentru aceasta operatorii trebuie să stabilească tipurile de acces după funcționalitate (cum ar fi: administrare, introducere, prelucrare, salvare etc.) și după acțiuni aplicate asupra datelor cu caracter personal (cum ar fi: scriere, citire, ștergere), precum și procedurile privind aceste tipuri de acces.

Programatorii sistemelor de prelucrare a datelor cu caracter personal nu vor avea acces la datele cu caracter personal. Operatorul va permite accesul programatorilor la datele cu caracter personal după ce acestea au fost transformate în date anonime.

Compartimentul care asigură suportul tehnic poate avea acces la datele cu caracter personal pentru rezolvarea unor cazuri excepționale.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Pentru activitatea de pregătire a utilizatorilor sau pentru realizarea de prezentări se vor folosi date anonime. Angajații care predau cursurile de pregătire vor folosi date cu caracter personal pe parcursul propriei lor pregătiri.

Operatorul va stabili modalitățile stricte prin care se vor distruge datele cu caracter personal. Autorizarea pentru această prelucrare de date cu caracter personal trebuie limitată la câțiva utilizatori.

Colectarea datelor

Operatorul desemnează utilizatori autorizați pentru operațiile de colectare și introducere de date cu caracter personal într-un sistem informațional.

Orice modificare a datelor cu caracter personal se poate face numai de către utilizatori autorizați desemnați de operator.

Operatorul va lua măsuri pentru ca sistemul informațional să înregistreze cine a făcut modificarea, data și ora modificării. Pentru o mai bună administrare operatorul va lua măsuri ca sistemul informațional să mențină datele șterse sau modificate.

Execuția copiilor de siguranță

Operatorul va stabili intervalul de timp la care se vor executa copiile de siguranță ale bazelor de date cu caracter personal, precum și ale programelor folosite pentru prelucrările automatizate. Utilizatorii care execută aceste copii de siguranță vor fi numiți de operator, într-un număr restrâns. Copiile de siguranță se vor stoca în alte camere, în fișete metalice cu sigiliu aplicat, și, dacă este posibil, chiar în camere din altă clădire.

Operatorul va lua măsuri ca accesul la copiile de siguranță să fie monitorizat.

Computerele și terminalele de acces

Computerele și alte terminale de acces vor fi instalate în încăperi cu acces restricționat. Dacă nu pot fi asigurate aceste condiții, computerele se vor instala în încăperi care se pot încuia sau se vor lua măsuri ca accesul la computere să se facă cu ajutorul unor chei ori

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

cartele magnetice.

Dacă pe ecran apar date cu caracter personal asupra cărora nu se acționează o perioadă dată, stabilită de operator, sesiunea de lucru trebuie închisă automat. Mărimea acestei perioade se determină în funcție de operațiile care trebuie executate.

Terminalele de acces folosite în relația cu publicul, pe care apar date cu caracter personal, vor fi poziționate astfel încât să nu poată fi văzute de public și după o perioadă scurtă, stabilită de operator, în care nu se acționează asupra lor, acestea trebuie ascunse.

Fișierele de acces

Operatorul este obligat să ia măsuri ca orice accesare a bazei de date cu caracter personal să fie înregistrată într-un fișier de acces (numit log la prelucrările automate) sau într-un registru pentru prelucrările manuale de date cu caracter personal, stabilit de operator. Informațiile înregistrate în fișierul de acces sau în registru vor fi:

- codul de identificare (numele utilizatorului pentru bazele de date cu caracter personal manuale);
- numele fișierului accesat (fișei);
- numărul înregistrărilor efectuate;
- tipul de acces;
- codul operației executate sau programul folosit;
- data accesului (an, lună, zi);
- timpul (ora, minutul, secunda).

Pentru prelucrările automate aceste informații vor fi stocate într-un fișier de acces general sau în fișiere separate pentru fiecare utilizator. Orice încercare de acces neautorizat va fi, de asemenea, înregistrată.

Operatorul este obligat să păstreze fișierele de acces cel puțin 2 ani, pentru a fi folosite ca probe în cazul unor investigații. Dacă investigațiile se prelungesc, aceste fișiere se vor păstra atât timp cât se va considera necesar.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Fișierele de acces trebuie să facă posibilă identificarea de către operator sau de către persoana împuternicită a persoanelor care au accesat date cu caracter personal fără un motiv anume, în vederea aplicării unor sancțiuni sau a sesizării organelor competente.

Sistemele de telecomunicații

Operatorul este obligat să facă periodic controlul autentificărilor și tipurilor de acces pentru detectarea unor disfuncționalități în ceea ce privește folosirea sistemelor de telecomunicații.

Operatorii sunt obligați să conceapă sistemul de telecomunicații astfel încât datele cu caracter personal să nu poată fi interceptate sau transmise de oriunde. Dacă sistemul de telecomunicații nu poate fi astfel securizat, operatorul este obligat să impună folosirea metodei de criptare pentru transmisia datelor cu caracter personal.

Prin sistemele de telecomunicații se vor transmite numai datele cu caracter personal strict necesare.

Instruirea personalului

În cadrul cursurilor de pregătire a utilizatorilor operatorul este obligat să facă informarea acestora cu privire la legislația pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, la cerințele minime de securitate a prelucrărilor de date cu caracter personal, precum și cu privire la riscurile pe care le comportă prelucrarea datelor cu caracter personal, în funcție de specificul activității utilizatorului.

Utilizatorii care au acces la date cu caracter personal vor fi instruiți de către operator asupra confidențialității acestora și vor fi avertizați prin mesaje care vor apărea pe monitoare în timpul activității. Utilizatorii sunt obligați să își închidă sesiunea de lucru atunci când părăsesc locul de muncă.

Folosirea computerelor

Pentru menținerea securității prelucrării datelor cu caracter personal (în special împotriva

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

virusilor informatici) operatorul va lua măsuri care vor consta în:

- a) interzicerea folosirii de către utilizatori a programelor software care provin din surse externe sau dubioase;
- b) informarea utilizatorilor în privința pericolului privind virusii informatici;
- c) implementarea unor sisteme automate de devirusare și de securitate a sistemelor informatice;
- d) dezactivarea, pe cât posibil, a tastei "Print screen", atunci când sunt afișate pe monitor date cu caracter personal, interzicându-se astfel scoaterea la imprimantă a acestora.

Imprimarea datelor

Scoaterea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatori autorizați pentru această operațiune de către operator. Operatorii sunt obligați să aprobe proceduri interne specifice privind folosirea și distrugerea acestor materiale.

Fiecare entitate își va aproba propriul sistem de securitate, ținând seama de aceste cerințe minime de securitate a prelucrărilor de date cu caracter personal, iar în funcție de importanța datelor cu caracter personal prelucrate, își va impune măsuri de securitate suplimentare.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Capitolul 8. Responsabilitatea

8.1. Evidența activităților de prelucrare

Regulamentul **obligă** operatorii și persoanele împuternicite să țină o evidență a activităților de prelucrare în următoarele situații:

- atunci când entitatea are *mai mult de 250 angajați*;
- *prelucrarea este susceptibilă să genereze un risc* pentru drepturile și libertățile persoanei vizate prelucrarea include categorii speciale de date;
- prelucrarea *nu este ocazională*.

Având în vedere că, în general, în activitatea unei firme, prelucrarea nu este ocazională, ar trebui ca fiecare organizație să aibă o evidență internă a activităților care să fie revizuită periodic.

👉 Acest registru intern va înlocui, începând cu 25 mai 2018, procedura notificării autorității de supraveghere cu privire la prelucrările de date.

Registruul va fi actualizat **periodic**, pe măsură ce intervin modificări (*de exemplu*: se colectează date suplimentare, se decide transferarea datelor către state terțe, se instituie măsuri suplimentare de securitate). Este recomandat să se stabilească revizuirea periodică a registruului (de exemplu, o dată pe lună) .

Registruul prelucrărilor poate constitui baza pentru redactarea notelor de informare către persoana vizată. Este recomandat să se păstreze o arhivă a versiunilor anterioare. Pe măsură ce intervin modificări în activitatea de prelucrare, persoana vizată va fi informată asupra modificărilor.

Ce trebuie să cuprindă obligatoriu evidența activităților de prelucrare a operatorului?

(a) numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

- (b) scopurile prelucrării;
- (c) o descriere a categoriilor de persoane vizate și 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 țări terțe sau organizații internaționale;
- (e) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale;
- (f) acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;
- (g) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 32 alineatul (1).⁶⁹

Ce trebuie să cuprindă obligatoriu evidența activităților de prelucrare a persoanei împuternicite?

- a) numele și datele de contact ale persoanei sau persoanelor împuternicite de operator și ale fiecărui operator în numele căruia acționează această persoană (aceste persoane), precum și ale reprezentantului operatorului sau al persoanei împuternicite de operator, după caz;
- b) categoriile de activități de prelucrare desfășurate în numele fiecărui operator;
- c) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective;
- d) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 32 alineatul (1).⁷⁰

8.2. Evaluarea impactului asupra protecției datelor (DPIA)

Atunci când, o anumită activitate de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile

⁶⁹ Art. (30) alin. (1) din Regulamentul (EU) 679/2016.

⁷⁰ Art. (30) alin. (2) din Regulamentul (EU) 679/2016.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

persoanelor fizice, operatorul efectuează, înainte de prelucrarea, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal.⁷¹

La realizarea unei evaluări a impactului asupra protecției datelor, operatorul solicită avizul responsabilului cu protecția datelor, dacă acesta a fost desemnat.⁷²

Evaluarea impactului este necesară mai ales atunci când:

- profilarea persoanelor produce efecte juridice semnificative sau afectează similar viața privată;
- prelucrării pe scară largă a unor categorii speciale de date sau a unor date cu caracter personal privind condamnări penale și infracțiuni; sau
- unei monitorizări sistematice pe scară largă a unei zone accesibile publicului. (CCTV, drone)⁷³

8.3. Responsabilul cu protecția datelor

Pe scurt

- ✚ Unele organizații vor fi obligate să desemneze un responsabil cu protecția datelor.
- ✚ În mod ideal, responsabilul cu protecția datelor ar trebui să fie ori un jurist care are cunoștințe de IT, ori un ITist care are cunoștințe juridice;
- ✚ Responsabilul cu protecția datelor nu poate fi demis pentru îndeplinirea activităților sale.
- ✚ Acesta poate să fie angajat sau externalizat, în temeiul unui contract de prestări servicii;

⁷¹ Art. (35) alin. (1) din Regulamentul (EU) 679/2016.

⁷² Art. (35) alin. (2) din Regulamentul (EU) 679/2016.

⁷³ Art. (35) alin. (3) din Regulamentul (EU) 679/2016.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

- ✚ Responsabilul cu protecția datelor nu poate fi o persoană din conducerea companiei, deoarece va un conflict de interese.

Responsabilul cu protecția datelor (DPO) va ajuta organizațiile să asigure respectarea prevederilor Regulamentului.

Este obligatoriu ca anumiți operatori și persoane împuternicite de operatori să desemneze un DPO .

Situațiile în care este obligatorie desemnarea unui DPO includ:

- Când prelucrarea este efectuată de o **autoritate publică sau un organism public**, cu excepția instanțelor care acționează în exercițiul funcției lor jurisdicționale;
- Dacă activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrarea care necesită o **monitorizare periodică și sistematică a persoanelor vizate pe scară largă**;
- Dacă activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în **prelucrarea pe scară largă** a unor categorii speciale de date sau a unor categorii de date cu caracter personal privind condamnări penale și infracțiuni.

Ce înseamnă „monitorizare periodică și sistematică”?

ANSPDCP spune că aceasta presupune „toate formele de urmărire și profilare pe Internet, inclusiv în scop de publicitate comportamentală, nefiind însă restricționată în mediul online. Sintagma ”periodică și sistematică” presupune o activitate continuă și recurentă, care implică prelucrări de date.”⁷⁴

Ce înseamnă prelucrarea „pe scară largă”?

ANSPDCP spune că, pentru a stabili dacă o prelucrare este pe scară largă, trebuie ținut

⁷⁴ http://www.dataprotection.ro/?page=Responsabilul_cu_protectia_datelor

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

cont de următoare:

- **numărul persoanelor vizate** – un număr exact ori un procent din populația relevantă;
- **volumul datelor și/sau gama** de elemente diferite de date în curs de prelucrare;
- **durata** sau **permanența** activității de prelucrare a datelor;
- **suprafața geografică** a activității de prelucrare.⁷⁵

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 de conținut, locație, trafic de către furnizorii de servicii de internet;

⁷⁵ idem

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

- prelucrarea datelor personale de către companii de asigurări;
- publicitate comportamentală.⁷⁶

Când nu este necesară desemnarea unui responsabil cu protecția 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.⁷⁷

👉 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.

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 calităților profesionale și, în special, a cunoștințelor de specialitate în dreptul și practicile din domeniul protecției datelor, precum și pe baza capacității de a îndeplini sarcinile prevăzute la articolul 39."⁷⁸

Responsabilul cu protecția datelor ar trebui să aibă următoarele **calități profesionale**:

- Cunoștințe de specialitate în dreptul și practicile din domeniul protecției datelor cu caracter personal și o înțelegere aprofundată a Regulamentului (EU)

⁷⁶ Idem.

⁷⁷ Idem.

⁷⁸ Idem.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

nr. 2016/679;

- Experiență relevantă în managementul protecției datelor cu caracter personal, proporțională cu sensibilitatea, complexitatea și volumul de date cu caracter personal pe care angajatorul le prelucrează;
- Integritate și etică profesională ridicată;
- Abilitatea de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale;
- Experiența relevantă în leadership și în gestionarea proiectelor;
- Abilitatea de a comunica eficient cu cele mai înalte niveluri ale conducerii;
- Abilitatea de a lua decizii în cadrul organizației;
- Abilitatea de a participa la elaborarea evaluărilor de impact asupra protecției datelor cu caracter personal, de a înțelege și evalua în mod adecvat riscurile;
- Înțelegerea standardelor internaționale de securitate a informației;
- Înțelegerea tehnologiei informației și a comunicațiilor, precum și practica și auditurile în materia securității informației;
- Abilitatea de a comunica în mod eficient cu persoanele vizate, cu Autoritățile de supraveghere, cu alți operatori, cu persoanele împuternicite, inclusiv la nivel internațional;
- Abilitatea de a conștientiza în mod adecvat situațiile, abilitatea de a-și recunoaște lacunele pentru a putea să-și îmbunătățească în mod constant cunoștințele, abilitatea de a identifica sursele de încredere pentru a se informa și a informa organizația în mod corespunzător;
- Cunoașterea în detaliu a proceselor organizatorice și administrative ale

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

companiei;

- Înțelegerea adecvată a operațiunilor de prelucrare, a sistemelor informatice și a cerințelor în materie de securitate și protecție a datelor cu caracter personal;
- Dorința de pregătire și perfecționare continuă;
- Abilitatea de a lua decizii și de a acționa independent.

Responsabilul cu protecția datelor ar trebui să aibă următoarele **atribuții**:

- Informarea, sfătuirea angajatorului și a celorlalți angajați, emiterea de recomandări către angajator, precum și către ceilalți angajați cu privire la obligațiile care le revin în temeiul Regulamentului (EU) 2016/679 și al altor dispoziții de drept al Uniunii sau drept intern referitoare la protecția datelor;
- Promovarea unei culturi a protecției datelor cu caracter personal în cadrul organizației;
- Organizarea de training-uri în vederea pregătirii și sensibilizării angajaților cu privire la prelucrarea datelor cu caracter personal;
- Participarea în mod regulat la ședințele conducerii unde se iau hotărâri cu implicații privind prelucrarea datelor și oferirea de opinii concrete și documentate;
- Colectarea informațiilor necesare pentru identificarea activităților de prelucrare;
- Colaborarea cu celelalte departamente precum HR, Juridic, IT, Securitate pentru a avea informațiile necesare îndeplinirii sarcinilor;
- Recomandări și sprijin concret în privința implementării cerințelor

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Regulamentului (EU) 2016/679, cum ar fi principiile prelucrării datelor, drepturile persoanei vizate, protecția datelor începând cu momentul conceperii și în mod implicit, păstrarea evidenței activităților de prelucrare, securitatea și managementul adecvat al incidentelor de securitate;

- Monitorizarea respectării Regulamentului, a altor dispoziții de drept al Uniunii sau de drept intern referitoare la protecția datelor;
- Monitorizarea respectării politicilor tehnice și organizaționale ale operatorului;
- Monitorizarea efectuării auditurilor necesare;
- Alocarea responsabilităților, sensibilizarea și formarea personalului implicat în operațiunile de prelucrare;
- Informarea organizației dacă este obligatorie sau necesară efectuarea unei evaluări de impact privind protecția datelor cu caracter personal, potrivit art. (35) din Regulament;
- Recomandări concrete în privința metodologiei care trebuie urmată pentru efectuarea unei evaluări de impact;
- În situația în care organizația nu dispune de resursele necesare pentru efectuarea internă a evaluării de impact, va recomanda externalizarea acestui proces și va îndruma organizația în alegerea corectă a persoanelor specializate care pot efectua evaluarea de impact;
- Recomandarea măsurilor care trebuie implementate (inclusiv politici tehnice și organizatorice) pentru a atenua orice riscuri la adresa drepturilor și intereselor persoanelor vizate;
- Sprijinirea conceperii și actualizării constante a evidenței activităților de prelucrare, potrivit art. (30) din Regulament;

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

- Cooperarea cu Autoritatea de Supraveghere;
- Asumarea rolului de punct de contact pentru Autoritatea de Supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menționată la articolul 36, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune;
- Asumarea rolului de punct de contact cu persoanele vizate privind toate chestiunile legate de prelucrarea datelor lor și la exercitarea drepturilor lor în temeiul Regulamentului;
- Oferirea de sprijin concret în situația unui incident de securitate și oferirea de sprijin cu privire la notificarea Autorității/Autorităților de Supraveghere competentă/competente și a persoanelor vizate;
- Respectarea secretului și a confidențialității în ceea ce privește îndeplinirea sarcinilor sale;
- Monitorizarea și oferirea de sprijin concret în orice alt aspect legat de protecția datelor cu caracter personal, conform dispozițiilor legale în vigoare.

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**.

Operatorul sau persoana împuternicită de operator, în ceea ce privește raporturile cu responsabilul cu protecția datelor, este **obligat** să:

- publice datele de contact ale responsabilului (adresă poștală, număr de telefon alocat special și/sau o adresă de email alocată special).
- comunice datele de contact ale responsabilului către Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

Responsabilului cu protecția datelor îi este permis să aibă și alte funcții.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Acestuia îi pot fi încredințate și alte sarcini și atribuții, cu condiția ca acestea să nu dea naștere unor **conflicte de interese** (*de exemplu*: nu poate fi director executiv, director operațional, director financiar, șeful serviciului medical, șeful departamentului de marketing, șeful departamentului de resurse umane sau șeful departamentului IT).

Responsabilul pentru protecția datelor **nu poate fi demis sau sancționat de operator sau persoana împuternicită de operator pentru îndeplinirea sarcinilor sale**. *De exemplu*, responsabilul nu poate fi demis pentru oferirea unui sfat conform sarcinilor sale.

Un responsabil cu protecția datelor ar putea fi totuși demis, în mod legal, din alte motive decât cele privind îndeplinirea sarcinilor sale în această calitate. *De exemplu*, responsabilul poate fi demis în caz de furt, hărțuire ori o abatere gravă similară.⁷⁹

⁷⁹ idem

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Capitolul 9. Transferurile internaționale

Pe scurt

- ✚ GDPR impune restricții privind transferul de date cu caracter personal în afara granițelor Uniunii Europene.
- ✚ Aceste restricții există pentru a se asigura că nivelul de protecție a datelor cu caracter personal nu este subminat.⁸⁰

Datele cu caracter personal **pot fi transferate în afara Uniunii Europene** în următoarele situații:

- Transferuri în temeiul unei decizii privind caracterul adecvat al nivelului de protecție;
- Transferuri în baza unor garanții adecvate;
- Reguli corporatiste obligatorii;
- Derogări pentru situații specifice.

Transferurile în temeiul unei decizii privind caracterul adecvat al nivelului de protecție

Transferul de date cu caracter personal către o țară terță sau o organizație internațională se poate realiza atunci când Comisia a decis că țara terță, un teritoriu ori unul sau mai multe sectoare specificate din acea țară terță sau organizația internațională în cauză asigură un nivel de protecție adecvat. Transferurile realizate în aceste condiții nu necesită autorizări speciale.⁸¹

⁸⁰<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/?template=pdf&patch=50>, accesat 05.05.2018.

⁸¹ Art. 45 din Regulamentul (EU) 679/2016.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Transferuri în baza unor garanții adecvate

Aceste garanții pot fi:

- un instrument obligatoriu din punct de vedere juridic și executoriu între autoritățile sau organismele publice;
- reguli corporatiste obligatorii;
- clauze standard de protecție a datelor adoptate de Comisie;
- clauze standard de protecție a datelor adoptate de o autoritate de supraveghere și aprobate de Comisie
- un cod de conduită aprobat
- un mecanism de certificare aprobat

Reguli corporatiste obligatorii

Autoritatea de supraveghere competentă aprobă reguli corporatiste obligatorii, cu **condiția** ca acestea:

- să fie obligatorii din punct de vedere juridic și să se aplice fiecărui membru vizat al grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună, inclusiv angajaților acestuia, precum și să fie puse în aplicare de membrii în cauză;
- să confere, în mod expres, drepturi opozabile persoanelor vizate în ceea ce privește prelucrarea datelor lor cu caracter personal;
- să îndeplinească anumite cerințe.⁸²

⁸² Art. 47 din Regulamentul (EU) 679/2016.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

Derogări pentru situații specifice

Dacă nu există o decizie privind caracterul adecvat al protecției, garanții adecvate sau reguli corporatiste obligatorii, un transfer de date internațional poate avea loc doar în următoarele cazuri:

- a) persoana vizată și-a exprimat în 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 și a unor garanții adecvate;
- b) transferul este necesar pentru executarea unui contract între persoana vizată și operator sau pentru aplicarea unor măsuri precontractuale adoptate la cererea persoanei vizate;
- c) transferul este necesar pentru încheierea unui contract sau pentru executarea unui contract încheiat în interesul persoanei vizate între operator și o altă persoană fizică sau juridică;
- d) transferul este necesar din considerente importante de interes public;
- e) transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanță;
- f) transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale altor persoane, atunci când persoana vizată nu are capacitatea fizică sau juridică de a-și exprima acordul;
- g) transferul se realizează dintr-un registru care, potrivit dreptului Uniunii sau al dreptului intern, are scopul de a furniza informații publicului și care poate fi consultat fie de public în general, fie de orice persoană care poate face dovada unui interes legitim, dar numai în măsura în care sunt îndeplinite condițiile cu privire la consultare prevăzute de dreptul Uniunii sau de dreptul intern în acel caz specific.

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la

<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple

**Implementează GDPR corect, complet și eficient cu
KIT-ul nostru de implementare disponibil pe
<https://legalup.ro/kit-gdpr/>**

Implementează GDPR corect, complet și eficient cu KIT-ul nostru de implementare disponibil la
<https://legalup.ro/kit-gdpr/>

#wemakeGDPRsimple