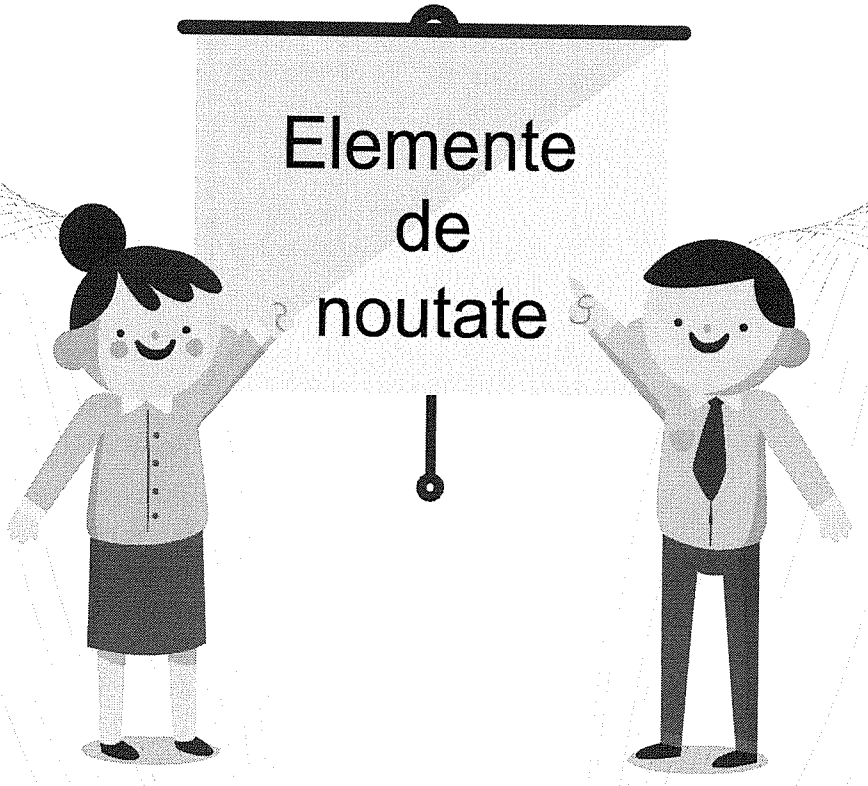
Noul Regulament General privind Protecţia Datelor



2018

ANS
PDCP

Regulamentul nr. 679/2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor)

Comisia Europeană a semnalat, în anul 2012, necesitatea actualizării cadrului normativ european aplicabil în domeniul protecţiei datelor şi a propus noi reguli utilizând ca instrument normativ regulamentul.

Regulamentul (UE) 2016/679 a intrat în vigoare pe 25 mai 2016, iar prevederile lui vor fi aplicabile începând cu data de 25 mai 2018.

Deşi principiile şi obiectivele principale stabilite de Directiva 95/46/CE rămân valabile, scopul principal al Regulamentului este acela de a adapta şi actualiza aceste principii în acord cu evoluţia tehnologiei.

Regulamentul stabileşte un set unic de reguli, direct aplicabile în toate statele membre ale Uniunii, destinat protejării mai eficiente a vieţii private a persoanelor fizice de pe teritoriul Uniunii Europene.

Principiile şi regulile stabilite de Regulament privesc un drept fundamental al persoanei – dreptul la protecţia datelor personale, garantat de art. 8 al Cartei Drepturilor Fundamentale a UE şi art. 16 al Tratatului UE.

Regulamentul accentuează responsabilitatea operatorilor care prelucrează date personale, simplificând, în acelaşi timp, formalităţile administrative pe care aceştia trebuie să le parcurgă.

Prevederile Regulamentului consolidează drepturile garantate persoanelor vizate (persoanele ale căror date sunt prelucrate).

Astfel, dreptul la informare este extins, în sensul că persoanele vizate pot obţine de la operatorul de date informaţii mai clare şi cuprinzătoare cu privire la scopul şi temeiul legal în care se prelucrează datele personale, perioada de stocare a acestora şi drepturile de care beneficiază.

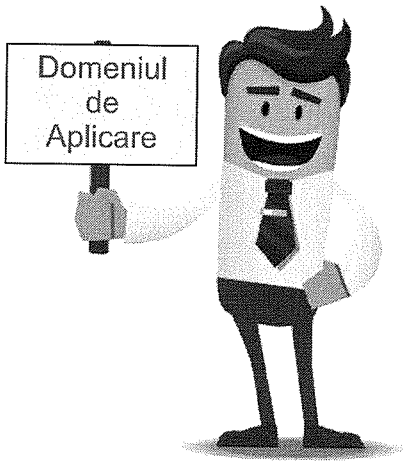
Dreptul de a fi uitat cu aplicabilitate în mediul on-line este consacrat expres.

Regulamentul mai prevede şi un drept nou, cel la portabilitatea datelor - mai exact posibilitatea persoanelor vizate de a cere transferarea datelor la un alt operator de date.

Minorii beneficiază de mai multă atenţie întrucât regulamentul stabileşte o serie de garanţii specifice pentru a proteja cât mai eficient viaţa privată a acestora, în special, în mediul on-line.

Regulile stabilite de Regulament vor fi aplicabile tuturor operatorilor de date, indiferent de locul unde sunt stabiliţi aceştia, în anumite condiţii.

Astfel, în măsura în care bunurile sau serviciile oferite de o companie aflată în afara UE, care presupun prelucrarea datelor personale, sunt adresate în mod vădit şi cetăţenilor Uniunii Europene, regulile stabilite de Regulament îi vor fi aplicabile şi acestei companii.



Domeniul de aplicare:

• este direct aplicabil în toate statele membre UE

• protejează drepturile tuturor persoanelor fizice aflate pe teritoriul UE, indiferent de situarea geografică a operatorului de date

• extinde sfera de aplicare şi asupra operatorilor de date stabiliţi în afara UE, în măsura în care bunurile şi/sau serviciile acestora sunt adresate (şi) persoanelor aflate pe teritoriul UE

Scopul Regulamentului este să contribuie la asigurarea unei zone de libertate, securitate şi justiţie pe teritoriul Uniunii Europene, o zonă în care este asigurat atât progresul economic şi social, cât şi binele individual.

Regulile şi principiile stabilite de Regulament protejează viaţa privată a tuturor persoanelor aflate pe teritoriul Uniunii Europene, ale căror date personale sunt prelucrate de companii /persoane fizice/instituţii/orice alte entităţi de drept public sau privat.

Aceste reguli şi principii sunt aplicabile tuturor persoanelor, indiferent de cetăţenia acestora sau de reşedinţă (în interiorul UE).

Operatorilor de date le este oferită posibilitatea de a interacţiona cu o singură autoritate de supraveghere, respectiv cea din statul membru în care este stabilit sediul principal al operatorului de date.

Regulamentul priveşte atât companiile aflate pe teritoriul Uniunii Europene, cât şi cele din afara acestui spaţiu care prelucrează, însă, date personale pentru a oferi bunuri şi servicii persoanelor aflate pe teritoriul Uniunii Europene, indiferent dacă bunurile şi serviciile respective sunt condiţionate sau nu de efectuarea unei plăţi.

Importantă este intenţia companiei de a oferi în mod efectiv bunuri şi/sau servicii persoanelor aflate pe teritoriul UE.

Pentru a identifica intenţia de a oferi bunuri sau servicii pe teritoriul Uniunii Europene sunt analizaţi mai mulţi factori, cum ar fi: utilizarea limbii oficiale a unuia dintre statele membre, posibilitatea de a plăti în euro sau altă monedă oficială a statelor membre ori de a livra produsele comandate pe teritoriul UE sau orice alte asemenea indicii.

De asemenea, Regulamentul va fi aplicabil şi companiilor aflate în afara Uniunii Europene în măsura în care prelucrarea de date efectuată presupune monitorizarea comportamentului persoanelor aflate pe teritoriul UE.

O astfel de monitorizare presupune, spre exemplu, urmărirea comportamentului în mediul on-line, inclusiv folosirea unor tehnici ulterioare de prelucrare a datelor cum ar fi crearea de profiluri. Astfel de tehnici sunt folosite pentru a stabili preferinţele persoanelor, comportamentele şi atitudinile acestora.

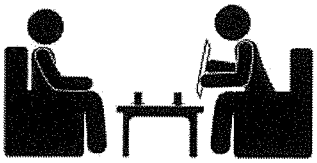
Excepţii:

• prevederile Regulamentului nu vor fi aplicabile prelucrărilor efectuate în scopul prevenirii, cercetării şi urmăririi penale a infractorului sau executarea sancţiunii penale. În cazul acestora vor fi aplicabile prevederile unei reglementări naţionale în aplicabilitatea Directivei (UE) 2016/680, (care face parte din acelaşi „pachet legislativ" cu Regulamentul UE 2016/679).

• Regulamentul nu va fi aplicabil activităţilor aflate în afara dreptului Uniunii – aici se încadrează şi prelucrările de date referitoare la securitatea naţională a statelor membre şi relaţiile externe.

• Regulamentul nu va fi aplicabil prelucrărilor de date efectuate de o persoană fizică în cadrul unei activităţi exclusiv personale.

• Activităţile cuprinse în ultima excepţie sunt unele strict personale şi exclud orice legătură cu profesia sau cu orice activitate comercială. Sunt incluse în această excepţie, spre exemplu, corespondenţa personală prin e-mail, socializarea în mediul on-line şi orice altă asemenea activitate.



Pentru persoanele vizate:

Sunt consolidate drepturile garantate persoanelor şi sunt introduse drepturi noi:

• **dreptul de a fi uitat** - persoanele fizice pot cere ştergerea datelor personale dacă acestea au fost prelucrate ilegal, fără consimţământul acestora sau dacă datele nu mai sunt necesare scopului în care au fost prelucrate iniţial.

În cazul dreptului de a fi uitat, a fost avută în vedere în special prelucrarea datelor în mediul on-line.

• Dreptul de a fi uitat nu este unul absolut – vor fi analizate întotdeauna circumstanţele specifice fiecărui caz în parte. Regulamentul permite păstrarea în continuare a datelor cu caracter personal în cazul în care aceasta este necesară pentru respectarea libertăţii de exprimare şi a dreptului la informare, pentru respectarea unei obligaţii legale, pentru îndeplinirea unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul, din motive de interes public în domeniul sănătăţii publice, în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice sau pentru constatarea, exercitarea sau apărarea unui drept în instanţă.

- **dreptul la portabilitatea datelor** - oferă posibilitatea persoanei fizice de a cere să se transmită datele la un alt operator sau de a primi datele personale care o privesc şi pe care le-a furnizat operatorului.

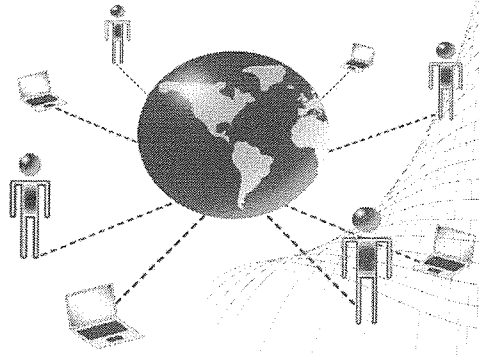
Operatorul de date trebuie să ofere datele într-un format structurat, utilizat în mod curent, prelucrabil automat şi interoperabil, tocmai pentru ca şi un alt operator de date să le poată prelucra ulterior.

Dreptul la portabilitatea datelor este aplicabil în măsura în care persoana vizată a oferit operatorului datele personale, iar acesta le prelucrează în baza consimţământului sau în executarea unui contract.

Nu se va putea exercita dreptul la portabilitatea datelor în cazul operatorilor de date care prelucrează datele persoanelor fizice în cadrul exercitării funcţiilor lor publice, în cazul în care prelucrarea este necesară în vederea respectării unei obligaţii legale căreia îi este supus operatorul ori în cazul îndeplinirii unei sarcini care serveşte unui interes public sau care rezultă din exercitarea unei autorităţi publice cu care este învestit operatorul de date.

În exercitarea dreptului la portabilitatea datelor, nu trebuie aduse atingeri drepturilor şi libertăţilor altor persoane – spre exemplu cazul unui set de date care priveşte mai multe persoane sau dreptul altei persoane de a obţine ştergerea datelor care o privesc.

Atunci când se exercită dreptul la portabilitatea datelor, operatorul de date poate transmite datele personale direct altui operator de date ales de persoana vizată.



Aspecte diverse:

Regulamentul stabileşte obligaţia operatorului de a demonstra obţinerea consimţământului persoanei pentru prelucrările de date personale. Persoana vizată are dreptul să îşi retragă în orice moment consimţământul, în situaţia în care acesta constituie temei de prelucrare a datelor.

Absenţa unei manifestări clare de acord nu poate fi privită ca o formă de exprimare a consimţământului. Spre exemplu, în cazul căsuţelor bifate (prin care este prestabilit acordul) nu poate fi prezumat un consimţământ exprimat în cunoştinţă de cauză.

În cazul în care datele sunt prelucrate în mai multe scopuri, este important ca operatorul de date să poată demonstra că a obţinut acordul persoanei pentru a-i prelucra datele în toate acele scopuri.

Regulamentul stabileşte obligaţia operatorului de date de a asigura un anumit nivel de transparenţă faţă de persoanele vizate. Acestea trebuie să ştie cine este operatorul de date, scopul în care le vor fi prelucrate datele, ce date sunt utilizate, ce drepturi le sunt garantate, cum îşi pot exercita aceste drepturi şi cine sunt/vor fi terţii cărora operatorul le va dezvălui datele, dacă este cazul.

În cazul în care sunt prelucrate date personale ale minorilor, operatorul de date trebuie să ofere informaţiile respective utilizând un limbaj cât mai simplu şi clar, astfel încât copilul/minorul să poată înţelege cu uşurinţă scopul şi modul în care îi vor fi prelucrate datele personale.

Proximitatea faţă de persoana vizată - autoritatea de supraveghere din statul membru în care se află persoana vizată acţionează ca interlocutor/punct de contact atunci când operatorul de date este stabilit într-un alt stat.

În cazul prelucrărilor de date care vizează persoane din mai multe state membre, fiecare persoană are posibilitatea de a se adresa (după caz, de a depune plângere) autorităţii de supraveghere din statul (membru UE) în care îşi are domiciliul/reşedinţa. În acest fel, este asigurată implicarea autorităţii de supraveghere din statul membru în care se află persoana în procedura de adoptare a unei decizii în cazul unui operator de date stabilit într-un alt stat membru.

Cooperare consolidată între autorităţile de supraveghere - în cazul prelucrărilor de date transnaţionale (cele care privesc persoane din mai multe state membre UE), autorităţii de supraveghere din statul respectiv îi sunt oferite competenţe pentru a se asigura, alături de autorităţile din celelalte state implicate, că datele sunt prelucrate conform regulilor şi principiilor stabilite de Regulament.

Pentru operatorii de date:

One stop shop - formalităţi reduse pentru operatorii de date (interlocutor unic la nivel UE).

Operatorii de date care îşi desfăşoară activităţile în mai multe state membre UE îşi pot alege un singur interlocutor - autoritatea de supraveghere din statul membru în care îşi au stabilit sediul principal.

Responsabilizarea operatorilor de date - accentul este pus pe transparenţa faţă de persoana vizată şi responsabilitatea operatorului de date faţă de modul în care prelucrează datele.

În cazul prelucrărilor de date care pot presupune un risc ridicat pentru viaţa privată a persoanelor, operatorul trebuie să efectueze un studiu de impact asupra vieţii private.

Rezultatul unui astfel de studiu îi va permite să identifice riscuri specifice şi să adopte măsuri care să împiedice apariţia / producerea acestor situaţii. Prelucrarea categoriilor de „date sensibile" poate presupune, de cele mai multe ori, apariţia unor riscuri specifice referitoare la viaţa privată a persoanelor.

O asemenea evaluare va începe întotdeauna cu inventarierea datelor/categoriilor de date personale pe care operatorul intenţionează să le prelucreze.

Acestea vor fi supuse unei analize de necesitate pentru a verifica dacă sunt, într-adevăr, necesare toate acele date/categorii de date pentru a atinge scopul urmărit de operator, în vederea respectării principiului minimizării datelor.

Ulterior pot fi identificate şi riscurile presupuse de prelucrarea acelor date, spre exemplu dezvăluirea neautorizată/accidentală/ilicită a datelor şi atingerile pe care producerea unui astfel de risc le pot aduce dreptului persoanei la viaţă privată.

În funcţie de riscurile identificate, operatorul de date îşi va stabili şi măsuri tehnice şi organizatorice (proceduri interne) pentru a preveni producerea acestora.

Privacy by design & Privacy by default - două principii esenţiale pentru operatorii de date.

Privacy by design - eşti dezvoltator de aplicaţii prin care se vor prelucra şi date personale? Trebuie să te asiguri, încă din stadiul dezvoltării, că aplicaţia ta va respecta regulile şi principiile stabilite de Regulament.

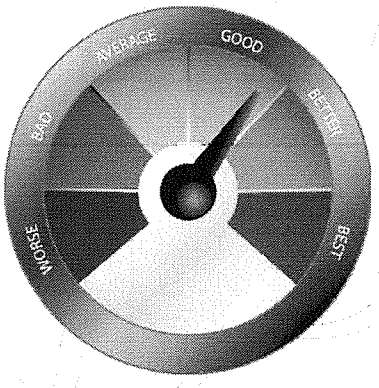
Privacy by default - furnizezi o aplicaţie care prelucrează date personale? Trebuie să te asiguri că setările iniţiale le vor permite utilizatorilor să îşi menţină controlul asupra vieţii lor private/ceea ce postează sau împărtăşesc cu alţi utilizatori. Utilizatorul poate alege să dezvăluie mai multe informaţii/date personale, însă trebuie să o facă în cunoştinţă de cauză, nu implicit (datorită setărilor iniţiale).

Transferul datelor în afara UE - atunci când datele personale sunt transferate în afara Uniunii Europene, acestea vor beneficia în continuare de nivelul de protecţie asigurat de regulile şi principiile stabilite de Regulament.

Operatorul de date utilizează unul dintre instrumentele prevăzute de Regulament:

- BCR - reguli corporatiste obligatorii
- clauze contractuale standard
- Decizii privind caracterul adecvat al nivelului de protecţie emise de către Comisia Europeană.

Pentru a se asigura nivelul de protecţie a datelor persoanelor fizice, transferul datelor cu caracter personal într-un stat terţ sau către o organizaţie internaţională se poate realiza doar cu respectarea unor condiţii de către operator şi persoana împuternicită de operator, inclusiv în ceea ce priveşte transferurile ulterioare de date din statul terţ către un alt stat terţ sau către o altă organizaţie internaţională.



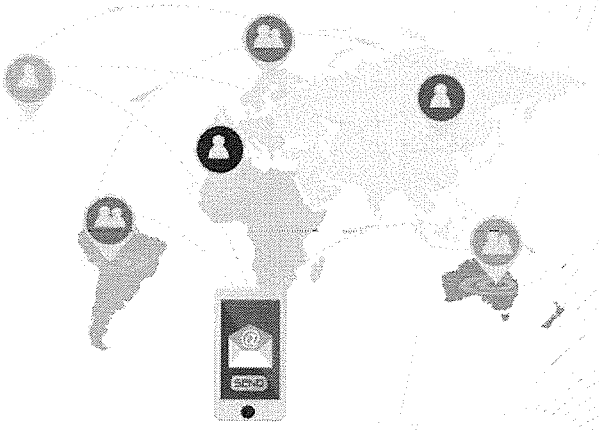
Transferul datelor cu caracter personal către un stat terţ, un teritoriu sau un sector specificat dintr-un stat terţ sau o organizaţie internaţională nu necesită autorizare atunci când Comisia Europeană a decis că statul terţ, teritoriul, sectorul specificat sau organizaţia internaţională oferă un nivel de protecţie adecvat.

În absenţa unei decizii privind caracterul adecvat al nivelului de protecţie, operatorul sau persoana împuternicită trebuie să adopte măsuri care să compenseze lipsa protecţiei datelor într-un stat terţ prin adoptarea unor garanţii eficiente pentru persoanele vizate, cum ar fi:

- un instrument obligatoriu din punct de vedere juridic şi executoriu între autorităţile sau organismele publice (acorduri administrative);
- reguli corporatiste obligatorii/ BCR (binding corporate rules);
- clauzele standard de protecţie a datelor adoptate de Comisia Europeană;
- clauzele standard de protecţie a datelor adoptate de autoritatea de supraveghere;
- un cod de conduită aprobat;
- un mecanism de certificare aprobat;
- clauze contractuale între operator sau persoana împuternicită de operator şi operatorul,persoana împuternicită de operator sau destinatarul datelor din statul terţ sau organizaţia internaţională;
- dispoziţii care urmează să fie incluse în acordurile administrative dintre autorităţile sau organismele publice, care includ drepturi opozabile şi efective pentru persoanele vizate (autorizaţia autorităţii competente ar trebui obţinută când garanţiile sunt oferite prin acorduri administrative fără caracter juridic obligatoriu).

Un transfer către un stat terţ sau o organizaţie internaţională mai poate avea loc, în absenţa unei decizii privind caracterul adecvat al nivelului de protecţie sau a unor garanţii adecvate, în una din următoarele condiţii:

- persoana vizată şi-a exprimat în mod explicit acordul cu privire la transferul propus;
- transferul este necesar pentru executarea unui contract între persoana vizată şi operator sau pentru aplicarea unor măsuri precontractuale adoptate la cererea persoanei vizate;
- transferul este necesar pentru încheierea unui contract sau pentru executarea unui contract încheiat în interesul persoanei vizate între operator şi o altă persoană fizică sau juridică;
- transferul este necesar din considerente importante de interes public;
- transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanţă;
- 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-şi exprima acordul;
- transferul se realizează dintr-un registru care, potrivit dreptului Uniunii sau dreptului intern, are scopul de a furniza informaţii publicului şi care poate fi consultat fie de public în general, fie de orice persoană care poate face dovada unui interes legitim, dar numai în condiţiile în care sunt îndeplinite condiţiile cu privire la consultare prevăzute de dreptul Uniunii Europene sau de dreptul intern în acel caz specific.



Responsabilul pentru protecţia datelor - DPO

Numirea unui responsabil pentru protecţia datelor la nivelul operatorului de date reprezintă una dintre măsurile prin care se încearcă responsabilizarea operatorilor de date.

Responsabilul pentru protecţia datelor oferă consultanţa necesară în vederea respectării tuturor obligaţiilor operatorului de date şi asigurării transparenţei necesare faţă de persoanele vizate.

Responsabilul pentru protecţia datelor poate oferi operatorului de date consultanţa necesară în vederea efectuării studiului de impact asupra vieţii private.

Operatorul de date trebuie să îşi desemneze un responsabil pentru protec?ia datelor în următoarele situaţii:

- atunci când operatorul de date este o autoritate publică (cu excepţia instanţelor sau a a autorităţilor judiciare);
- în cazul în care activitatea principală a operatorului de date constă în operaţiuni de prelucrare care necesită o monitorizare regulată şi sistematică a persoanelor vizate pe scară largă;
- în cazul în care activitatea principală a operatorului de date (sau a împuternicitului acestuia) constă în prelucrarea pe scară largă de categorii speciale de date cu caracter personal şi de date privind condamnările penale şi infracţiunile.

Este recomandată numirea unui responsabil pentru protecţia datelor la nivelul operatorului de date şi în afara cazurilor de mai sus, întrucât în acest fel poate fi asigurată respectarea prevederilor Regulamentului în cadrul prelucrării de date efectuată de către operatorul de date / împuternicitul acestuia.

Sancţiuni severe - până la 10 – 20 milioane de euro sau între 2% şi 4% din cifra de afaceri la nivel internaţional, pentru operatorii din sectorul privat.

Regulamentul stabileşte criterii clare de individualizare a sancţiuni – vor fi avute în vedere în mod corespunzător natura, gravitatea şi durata încălcării, caracterul deliberat al încălcării, acţiunile întreprinse pentru a reduce prejudiciul cauzat, gradul de răspundere sau orice încălcări anterioare relevante, modul în care încălcarea a fost adusă la cunoştinţa autorităţii de supraveghere, conformitatea cu măsurile adoptate împotriva operatorului sau a persoanei împuternicite de operator, aderarea la un cod de conduită şi orice alt factor agravant sau atenuant.

Fiecare stat membru poate prevedea norme prin care să se stabilească dacă şi în ce măsură pot fi impuse amenzi autorităţilor publice.

Bulevardul G-ral Gheorghe Magheru 28-30, sector 1
Bucureşti, cod poştal 010336
Telefon : 031.805.9211
Fax : 031.805.9602
E-mail : anspdcp@dataprotection.ro
Web : www.dataprotection.ro

ANS
PDCP

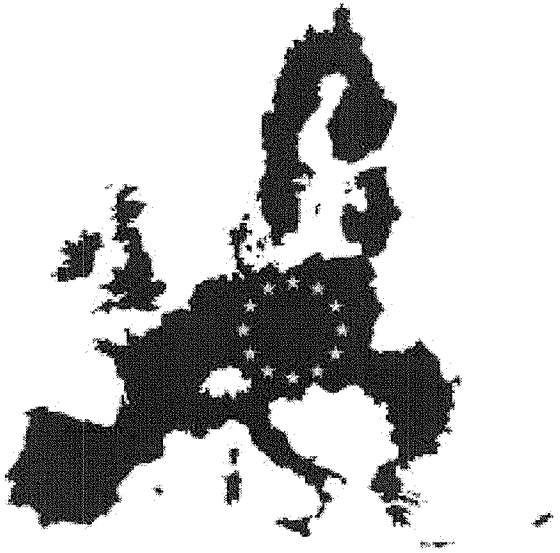
AUTORITATEA NAŢIONALĂ
DE SUPRAVEGHERE A PRELUCRĂRII
DATELOR CU CARACTER PERSONAL

- este autoritate publică centrală, autonomă şi independentă.

Scop:

- apărarea dreptului la viaţă intimă, familială şi privată în privinţa prelucrării datelor cu caracter personal.

AUTORITATEA NAŢIONALĂ
DE SUPRAVEGHERE A PRELUCRĂRII
DATELOR CU CARACTER PERSONAL



Blvd. G-ral Gheorghe Magheru nr. 28-30, sector 1, Bucureşti, cod postal 010336
Telefon: 031.805.9211
Fax.: 031.805.9602
www.dataprotection.ro
E-mail:anspdcp@dataprotection.ro

AUTORITATEA NAŢIONALĂ
DE SUPRAVEGHERE A PRELUCRĂRII
DATELOR CU CARACTER PERSONAL

Regulament (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE

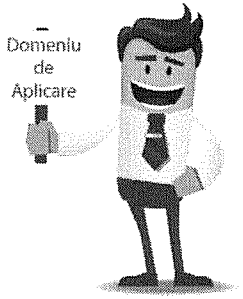
Bucureşti

Regulament general privind protecţia datelor

Context:

Regulamentul (UE) 2016/679 a fost adoptat de Parlamentul European şi Consiliu în data de 27 aprilie 2016, a fost publicat în Jurnalul Oficial Uniunii L119 din 4 mai 2016, iar prevederile lui vor fi aplicabile începând cu data de 25 mai 2018.

Regulamentul general privind protecţia datelor impune un set unic de reguli, direct aplicabile în toate statele membre ale Uniunii şi înlocuieşte Directiva 95/46/CE şi, implicit, prevederile Legii nr. 677/2001.



Domeniu de aplicare:

- este direct aplicabil în toate statele membre UE

- protejează drepturile tuturor persoanelor aflate pe teritoriul UE, indiferent de poziţionarea geografică a operatorului de date

- extinde sfera de aplicare şi asupra operatorilor de date stabiliţi în afara UE, în măsura în care bunurile şi/sau serviciile acestora sunt adresate (şi) persoanelor aflate pe teritoriul UE; ace?ti operatori de date vor trebui să respecte regulile şi principiile stabilite de Regulament

Pentru persoanele vizate:

Sunt garantate drepturi noi:

- **dreptul de a fi uitat** - se poate cere ştergerea datelor dacă acestea sunt prelucrate ilegal, fără consimţământ sau dacă datele nu mai sunt necesare scopului în care au fost prelucrate iniţial

- **dreptul la portabilitatea datelor** - există mai multă libertate de alegere. Se poate opta pentru transmiterea de date la un alt operator

Prevederi specifice referitoare la minori - sunt necesare reguli clare şi simple pe care tânărul / copilul să le înţeleagă şi trebuie obţinut consimţământul părintelui / tutorelui, după caz

Proximitatea faţă de persoana vizată - autoritatea de supraveghere din statul membru în care se află persoana vizată acţionează ca punct de contact atunci când operatorul reclamat este stabilit într-un alt stat

Cooperare consolidată între autorităţile de supraveghere - în cazul prelucrărilor de date transnaţionale (cele care privesc persoane din mai multe state membre UE), Regulamentul oferă autorităţii de supraveghere din statul tău competenţe pentru a se asigura, alături de autorităţile din celelalte state implicate, că datele tale sunt prelucrate conform regulilor şi principiilor stabilite de acesta

Pentru operatorii de date:

One stop shop - pentru operatorii de date care îşi desfăşoară activităţile în mai multe state membre UE, autoritatea de supraveghere competentă este cea din statul membru în care operatorul respectiv îşi are stabilit sediul principal

Responsabilizarea operatorilor de date - accentul este pus pe transparenţa faţă de persoana vizată şi responsabilitatea operatorului de date faţă de modul în care sunt prelucrate datele

Studiu de impact - în cazul prelucrărilor de date care presupun un risc ridicat pentru viaţa privată a persoanelor, operatorul trebuie să efectueze un Studiu de Impact asupra vieţii private. Rezultatul unui astfel de studiu îi va permite să identifice riscuri specifice şi să adopte măsuri care să împiedice apariţia / producerea acestor situaţii

Transferul datelor în afara UE - pentru transferul datelor în afara Uniunii, Regulamentul introduce instrumente noi, pe lângă cele consacrate deja: BCR, clauze contractuale standard şi Decizii ale Comisiei Europene privind un nivel adecvat de protecţie

Privacy by design & Privacy by default - două noi principii esenţiale pentru operatorii de date

Privacy by design - eşti dezvoltator de aplicaţii (care vor prelucra şi date personale)? Trebuie să te asiguri, încă din stadiul dezvoltării, că aplicaţia ta va respecta regulile şi principiile stabilite de Regulament

Privacy by default - furnizezi o aplicaţie care prelucrează date personale? Trebuie să te asiguri că setările iniţiale le vor permite utilizatorilor să îşi menţină controlul asupra vieţii lor private / asupra a ceea ce postează sau împărtăşesc cu alţi utilizatori

DPO - data protection officer / responsabilul pentru protecţia datelor

Numirea unui DPO la nivelul operatorului de date reprezintă una dintre măsurile prin care se încearcă responsabilizarea operatorilor de date. Acesta oferă operatorului consultanţa necesară în vederea respectării tuturor obligaţiilor acestuia şi asigurării transparenţei necesare faţă de persoanele vizate.

Sancţiuni severe - până la 10 – 20 milioane de euro sau între 2% şi 4% din cifra de afaceri la nivel internaţional.

AUTORITATEA NAȚIONALĂ DE SUPRAVEGHERE

A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

GHID

ÎNTREBĂRI ȘI RĂSPUNSURI CU PRIVIRE LA APLICAREA REGULAMENTULUI (UE) 2016/679

romania2019.eu
Președinția României la Consiliul Uniunii Europene

ANS
PDCP

Notes

1. Care este domeniul de aplicare a Regulamentului (UE) 2016/679?

Regulamentul (UE) 2016/679 se aplică prelucrării datelor cu caracter personal, efectuată total sau parţial prin mijloace automatizate, precum şi prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidenţă a datelor sau care sunt destinate să facă parte dintr-un sistem de evidenţă a datelor.

Regulamentul (UE) 2016/679 se aplică prelucrării datelor cu caracter personal în cadrul activităţilor unui sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii.

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

- oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăţi de către persoana vizată; sau
- monitorizarea comportamentului persoanelor vizate dacă acesta se manifestă în cadrul Uniunii.

(art. 2 și art 3 din RGPD)

2. Când nu se aplică Regulamentul (UE) 2016/679?

Regulamentul (UE) 2016/679 **nu se aplică** prelucrării datelor cu caracter personal:

- *în cadrul unei activități care nu intră sub incidența dreptului Uniunii*;
- *de către statele membre atunci când desfășoară activități legate de politica externă și de securitatea comună a Uniunii*;
- *de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice*;
- *de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor, al executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora*; acestea sunt reglementate de **Directiva (UE) 2016/680** a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului, care a fost implementată prin Legea nr. 363/2018 privind protecţia persoanelor fizice referitor la

prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracţiunilor sau al executării pedepselor, măsurilor educative şi de siguranţă, precum şi privind libera circulaţie a acestor date.

(art. 2 din RGPD)

3. Regulamentul (UE) 2016/679 se aplică prelucrărilor efectuate de persoane fizice pentru uz personal?

Regulamentul general privind protecția datelor (RGPD) **nu se aplică** prelucrării datelor cu caracter personal efectuate de către **o persoană fizică în cadrul unei activități exclusiv personale sau domestice.**

În considerentul 18 din RGPD se precizează că activitățile personale sau domestice nu ar trebui să aibă legătură cu activtatea profesională sau comercială. Activitățile personale sau domestice pot include *corespondența și repertoriul de adrese sau activitățile din cadrul rețelelor sociale și activitățile online desfășurate în contextul respectivelor activități.*

(art. 2 din RGPD)

4. Regulamentul (UE) 2016/679 se aplică prelucrărilor efectuate de autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, precum și privind libera circulație a acestor date?

Regulamentul general privind protecția datelor nu se aplică prelucrărilor efectuate de autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, precum și privind libera circulație a acestor date.

Aceste prelucrări sunt reglementate de Legea nr. 363/2018 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, precum și privind libera circulație a acestor date, **act normativ care a transpus Directiva (UE) 2016/680 a** Parlamentului European și a Consiliului din 27 aprilie 2016.

Prelucrarea datelor cu caracter personal pentru realizarea activităților de menținere și asigurare a ordinii și siguranței publice ***se realizează numai dacă acestea sunt prevăzute de lege și sunt necesare pentru prevenirea unui pericol cel puțin asupra vieții, integrității corporale***

sau sănătăţii unei persoane ori a proprietăţii acesteia, precum şi pentru combaterea infracţiunilor.

Legea nr. 363/2018 ***nu se aplică*** *prelucrărilor de date cu caracter personal efectuate pentru realizarea activităţilor din domeniul apărării naţionale şi securităţii naţionale, în limitele şi cu restricţiile stabilite prin legislaţia în materie.*

(art. 2 din RGPD)

5. Ce înseamnă operator de date cu caracter personal?

Operator înseamnă 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. Atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, ***operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern.***

(art. 4 din RGPD)

6. Ce înseamnă operatori asociați?

Operatori asociați sunt doi sau mai mulți operatori care stabilesc în comun scopurile și mijloacele de prelucrare.

Operatorii asociați stabilesc într-un mod transparent responsabilitățile fiecăruia în ceea ce privește îndeplinirea obligațiilor care le revin în temeiul Regulamentului, în special în ceea ce privește exercitarea drepturilor persoanelor vizate și îndatoririle fiecăruia de furnizare a informațiilor prevăzute la articolele 13 și 14, prin intermediul *unui acord* între ei, cu excepția cazului și în măsura în care responsabilitățile operatorilor sunt stabilite în dreptul Uniunii sau în dreptul intern care se aplică acestora.

(art. 26 din RGPD)

7. Ce înseamnă persoană împuternicită de operator?

Persoana împuternicită de operator înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului.
Prelucrarea datelor efectuată de către o persoană împuternicită de operator este reglementată de art. 28 din RGPD.

(art. 4 și art. 28 din RGPD)

8. Este necesar să notific Autorității Naționale de Supraveghere prelucrările de date?

Având în vedere faptul că începând cu data de 25 mai 2018 se aplică Regulamentul (UE) 2016/679, operatorii nu mai au obligația de notificare a prelucrărilor de date.

În consecință, *Registrul on-line de evidență a prelucrărilor de date cu caracter personal* nu mai este disponibil pe site-ul autorității de supraveghere. De asemenea, nu se mai impune utilizarea numărului de notificare acordat în baza Legii nr. 677/2001.

9. Ce obligaţii am în calitate de operator potrivit Regulamentului (UE) 2016/679?

Obligațiile pe care le au operatorii de date cu caracter personal sunt reglementate în Capitolul IV din Regulamentul (UE) 2016/679.

Printre principalele obligații ale operatorului în aplicarea Regulamentului se numără:

- respectarea principiilor de prelucrare a datelor (art. 5 din Regulament);
- respectarea drepturilor persoanelor fizice (art. 12-23 din Regulament);
- asigurarea securității datelor (art. 25 și art. 32 din Regulament);
- desemnarea unui responsabil cu protecția datelor (art. 37-39 din Regulament), după caz;
- notificarea încalcărilor de securitate (art. 33 din Regulament), după caz;
- evaluarea impactului asupra protecției datelor și respectarea drepturilor persoanelor fizice (art. 35 din Regulament), după caz;
- cartografierea prelucrărilor de date cu caracter personal (art. 30 din Regulament).

Pentru mai multe informații se poate accesa *Ghidul orientativ de aplicare a Regulamentului general privind protecția datelor* emis de Autoritatea Națională de Supraveghere.

Pot fi accesate și următoarele ghiduri emise de Comitetul European pentru Protecția Datelor:

- *Ghidul privind responsabilul pentru protecția datelor;*
- *Ghidul privind evaluarea de impact;*
- *Ghidul privind notificarea încălcărilor de securitate;*
- *Ghidul privind dreptul la portabilitatea datelor;*
- *Ghidul privind deciziile automate individuale și profilare;*
- *Ghidul privind transparența*;
- *Ghidul privind consimțământul.*

10. Ce obligaţii am în calitate de persoană împuternicită de operator?

În cazul în care prelucrarea urmează să fie realizată în numele unui operator, acesta recurge doar la persoane împuternicite care oferă garanţii suficiente pentru punerea în aplicare a unor măsuri tehnice şi organizatorice adecvate, astfel încât prelucrarea să respecte cerinţele prevăzute în Regulament şi să asigure protecţia drepturilor persoanei vizate (art. 28 din Regulament).

Prelucrarea efectută de către o persoană împuternicită în numele unui operator este reglementată printr-un contract sau alt act juridic în temeiul dreptului Uniunii sau al dreptului intern care are caracter obligatoriu pentru persoana împuternicită de operator în raport cu operatorul şi care stabileşte *obiectul şi durata prelucrării, natura şi scopul prelucrării, tipul de date cu caracter personal şi categoriile de persoane vizate şi obligaţiile şi drepturile operatorului.*

(art. 28 din RGPD)

11. Ce trebuie să prevadă contractul sau actul juridic încheiat între operator şi persoana împuternicită de operator?

Contractul sau actul juridic prevede în special că persoană împuternicită de operator:

- prelucrează datele cu caracter personal numai pe baza unor instrucţiuni documentate din partea operatorului, inclusiv în ceea ce priveşte transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, cu excepţia cazului în care această obligaţie îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică;
- se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidenţialitatea sau au o obligaţie statutară adecvată de confidenţialitate;
- adoptă măsuri tehnice și organizatorice adecvate;
- respectă condiţiile privind recrutarea unei alte persoane împuternicite de operator;
- oferă asistenţă operatorului prin măsuri tehnice şi organizatorice adecvate, în măsura în care acest lucru este posibil, pentru îndeplinirea obligaţiei operatorului de a răspunde cererilor privind exercitarea de către persoana vizată a drepturilor sale;
- ajută operatorul să asigure respectarea obligaţiilor pe care acesta le are, în aplicarea Regulamentului;
- şterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare şi elimină copiile

existente, cu excepţia cazului în care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal;
- pune la dispoziţia operatorului toate informaţiile necesare pentru a demonstra respectarea obligaţiilor sale, permite desfăşurarea auditurilor, inclusiv a inspecţiilor, efectuate de operator sau alt auditor mandatat şi contribuie la acestea.

(art. 28 din RGPD)

12. Când desemnez un reprezentant al operatorului sau al persoanei împuternicite de operator?

Operatorul sau persoana împuternicită de operator care nu este stabilit(ă) în Uniunea Europeană are obligaţia de a desemna un reprezentant în Uniune atunci când prelucrează date caracter personal ale unor persoane vizate care se află în Uniune în legătură cu:
- ***oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăți de către persoana vizată; sau***
- ***monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Uniunii (art. 27 din Regulament).***

(art. 27 din RGPD)

13. Când trebuie să desemnez un responsabil cu protecţia datelor (DPO)?

Desemnarea responsabilului cu protecţia datelor este obligatorie atunci când:
- prelucrarea este efectuată de o autoritate sau un organism public, cu excepţia instanţelor care acţionează în exerciţiul funcţiei lor jurisdicţionale;
- Autorităţile şi organismele publice sunt: *Camera Deputaţilor şi Senatul, Administraţia Prezidenţială, Guvernul, ministerele, celelalte organe de specialitate ale administraţiei publice centrale, autorităţile şi instituţiile publice autonome, autorităţile administraţiei publice locale şi deja nivel judeţean, alte autorităţi publice, precum şi instituţiile din Subordinea/coordonarea acestora; de asemenea, sunt asimilate autorităţilor/organismelor publice şi unităţile de cult şi asociaţiile şi fundaţiile de utilitate publică* - art. 2 alin. (1) lit. a) şi art. 10 din Legea nr. 190/2018.
- activităţile principale ale operatorului sau ale persoanei împuternicite de operator constau în operaţiuni de prelucrare care, prin natura, domeniul

de aplicare și/sau scopurile lor, necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă;

- activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date sau a unor date cu caracter personal privind condamnări penale și infracțiuni (art. 37 alin. (1) din Regulament);
- în alte cazuri decât cele mai sus menţionate, operatorul sau persoana împuternicită de operator ori asociaţiile şi alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori pot desemna sau, acolo unde dreptul Uniunii sau dreptul intern solicită acest lucru, desemnează un responsabil cu protecţia datelor. Responsabilul cu protecţia datelor poate să acţioneze în favoarea unor astfel de asociaţii şi alte organisme care reprezintă operatori sau persoane împuternicite de operatori.

Pentru mai multe informații puteți accesa *Ghidul privind responsabilul cu protecția datelor* emis de Comitetul European pentru Protecția Datelor.

(art. 37 din RGPD)

14. Ce înseamnă prelucrare pe scară largă?

Atunci când se stabilește dacă prelucrarea este efectuată pe scară largă, trebuie să fie luați în considerare următorii factori:

- **numărul persoanelor vizate** (ori 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.

Pentru mai multe informații puteți accesa *Ghidul privind responsabilul cu protecția datelor* emis de Comitetul European pentru Protecția Datelor.

15. Ce condiții trebuie să îndeplinească responsabilul cu protecția datelor?

Responsabilul cu protecţia datelor este desemnat pe baza:
calităţilor profesionale, în special, a cunoştinţelor de specialitate în dreptul şi practicile din domeniul protecţiei datelor;
capacităţii de a-şi îndeplini sarcinile.

Pentru mai multe informații puteți accesa *Ghidul privind responsabilul cu protecția datelor* emis de Comitetul European pentru Protecția Datelor.

(art. 37 din RGPD)

16. Se poate desemna un singur responsabil cu protecția datelor pentru un grup de întreprinderi sau pentru mai multe autorități sau organisme publice?

Un grup de întreprinderi poate desemna un responsabil cu protecția datelor unic, cu condiția ca acesta să fie ușor accesibil din fiecare întreprindere.

Noțiunea de accesibilitate se referă la sarcinile responsabilului cu protecția datelor ca punct de contact în ceea ce privește persoanele vizate, autoritatea de supraveghere, dar și pe plan intern în cadrul organizației.

De asemenea, *mai multe autorități sau organisme publice* pot desemna un responsabil cu protecția datelor unic, luând în considerare structura organizatorică și dimensiunea acestora.

Pentru mai multe informații puteți accesa *Ghidul privind responsabilul cu protecția datelor* emis de Comitetul European pentru Protecția Datelor.

17. Cum comunic responsabilul cu protecția datelor autorității de supraveghere?

Operatorul sau persoana împuternicită de operator are obligația de a publica datele de contact ale responsabilului cu protecția datelor și de a le comunica autorității de supraveghere.

Comunicarea responsabilului cu protecția datelor se realizează prin *completarea on-line* a formularului de declarare a responsabilului cu protecția datelor existent pe site-ul Autorității www.dataprotection.ro, la Secțiunea „Responsabilul cu protecția datelor", urmată de accesarea butonului "Trimite chestionarul".

În situația în care un *grup de întreprinderi sau mai multe autorități sau organisme publice* desemnează un responsabil cu protecția datelor unic, fiecare operator sau persoană împuternicită va completa formularul de declarare a responsabilului cu protecția datelor existent pe site-ul Autorității, la Secțiunea „Responsabilul cu protecția datelor".

18. Cum modific datele responsabilului cu protecția datelor din formularul on-line transmis autorității de supraveghere?

În situația în care intervin modificări/completări în ceea ce privește informațiile cuprinse în formularul de declarare a responsabilului cu protecția datelor, este necesar să se completeze și să se transmită autorității de supraveghere un nou formular în același mod descris la punctul 17.

19. Care sunt condițiile legale de prelucrare a datelor cu caracter personal, altele decât datele cu caracter special?

Prelucrarea este legală numai dacă și în masura în care se aplică cel puțin una din următoarele condiții:

- când persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale pentru unul sau mai multe scopuri specifice;
- când prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;
- când prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;
- când prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;
- când prelucrarea este necesară pentru îndeplinira unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;
- când prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil (nu se aplică în cazul prelucrării efectuate de autorități publice în îndeplinirea atribuțiilor lor).

(art. 6 din RGPD)

20. Care sunt condițiile de prelucrare a datelor cu caracter special?

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 este interzisă.

Prelucrarea acestor categorii de date este permisă numai în următoarele condiții:

- ✓ persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice;
- ✓ prelucrarea este necesară în scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă și al securității sociale și protecției sociale;

- ✓ 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;
- ✓ prelucrarea este efectuată în cadrul activităților lor legitime și cu garanții adecvate de către o fundație, o asociație sau orice alt organism fără scop lucrativ și cu specific politic, filozofic, religios sau sindical;
- ✓ prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;
- ✓ prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare;
- ✓ prelucrarea este necesară din motive de interes public major, în baza dreptului UE sau a dreptului intern;
- ✓ 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;
- ✓ prelucrarea este necesară din motive de interes public în domeniul sănătății publice, cum ar fi protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale;
- ✓ prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice.
- ✓ Prelucrarea datelor genetice, biometrice sau a datelor privind sănătatea, în scopul realizării unui proces decizional automatizat sau pentru crearea de profiluri, este permisă cu consimţământul explicit al persoanei vizate sau dacă prelucrarea este efectuată în temeiul unor dispoziţii legale exprese, cu instituirea unor măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate.

(art. 9 din RGPD și art. 3 din Legea nr. 190/2018)

21. Care sunt condițiile de acordare și valabilitate a consimțământului?

Consimțământul persoanei vizate trebuie acordat printr-o acțiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoștință de cauză și clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal, cum ar fi:

- declarație făcută în scris într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu;
- declarație în format electronic - bifarea unei căsuțe atunci când persoana vizitează un site;
- declarație exprimată verbal.

Absența unui răspuns, căsuțele bifate în prealabil sau absența unei acțiuni nu constituie un consimțământ.

Consimțământul trebuie să vizeze toate activitățile de prelucrare efectuate în același scop sau în aceleași scopuri. Dacă prelucrarea datelor se face în mai multe scopuri, consimțământul trebuie dat pentru toate scopurile prelucrării.

Operatorul trebuie să fie în măsură să demonstreze faptul că persoana vizată și-a dat consimțământul pentru operațiunea de prelucrare a datelor cu caracter personal.

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

Pentru mai multe informații puteți accesa *Ghidul privind consimțământul* emis de Comitetul European pentru Protecția Datelor.

22. Dacă prelucrarea altor date decât cele cu caracter special este necesară în vederea îndeplinirii unei obligații legale care îmi revine ca operator, mai este necesar să obțin consimțământul persoanelor vizate?

Atunci când prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului, nu mai este necesară obținerea consimțământului persoanelor vizate (de exemplu, prelucrarea datelor angajaților de către angajator în vederea transmiterii acestora către REVISAL).

Pentru mai multe informații puteți accesa *Ghidul privind consimțământul* emis de Comitetul European pentru Protecția Datelor.

23. Care sunt condițiile pentru retragerea consimțământului?

Retragerea consimțământului persoanei vizate trebuie să se realizeze cu respectarea anumitor condiții, cum ar fi:

Operatorul trebuie să se asigure că persoana vizată poate să-și retragă consimțământul cu aceeași ușurință cu care l-a acordat și în orice moment;

Persoana vizată ar trebui să își poată retrage consimțământul fără a fi prejudiciată;

Operatorul trebuie să facă posibilă retragerea consimțământului în mod gratuit sau fără scăderea calității serviciului;

Operatorul trebuie să informeze persoana vizată asupra dreptului de retragere a consimțământului înainte de acordarea efectivă a consimțământului.

În cazul retragerii consimțământului, toate operațiunile de prelucrare a datelor care s-au bazat pe consimțământul respectiv și au avut loc înainte de retragerea acestuia și în conformitate cu Regulamentul (UE) 2016/679, *continuă să fie legale*, însă operatorul trebuie să oprească acțiunile de prelucrare în cauză. Dacă nu există un alt temei legal care să justifice prelucrarea datelor, acestea ar trebui să fie șterse de către operator.

Pentru mai multe informații puteți accesa *Ghidul privind consimțământul* emis de Comitetul European pentru Protecția Datelor.

(art. 7 din RGPD)

24. În ce condiții se pot prelucra datele cu caracter personal ale copiilor în ceea ce privește oferirea de servicii ale societății informaționale?

Prelucrarea datelor cu caracter personal ale unui copil, efectuată în baza **consimțământului** acestuia, este legală doar atunci când acesta are **cel puțin vârsta de 16 ani**.

Dacă copilul are **sub vârsta de 16 ani**, respectiva prelucrare este legală numai dacă și în măsura în care **consimțământul este acordat sau autorizat de titularul răspunderii părintești** asupra copilului.

Operatorul depune toate eforturile rezonabile pentru a verifica în astfel de cazuri că titularul răspunderii părintești a acordat sau a autorizat consimțământul, ținând seama de tehnologiile disponibile (art. 8 din Regulamentul (UE) 2016/679).

Pentru mai multe informații puteți accesa *Ghidul privind consimțământul* emis de Comitetul European pentru Protecția Datelor.

(art. 8 din RGPD)

25. Operatorii sau persoanele împuternicite de operatori trebuie să țină o evidență a prelucrărilor de date?

Fiecare operator sau persoană împuternicită trebuie să păstreaze, atât în scris cât și în format electronic, o evidență a activităților de prelucrare.

Evidența prelucrării cuprinde toate următoarele informații:

- numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;
- scopurile prelucrării;
- descriere a categoriilor de persoane vizate și a categoriilor de date cu

caracter personal;

- categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale;
- dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională;
- termenele-limită preconizate pentru ștergerea diferitelor categorii de date;
- descrierea generală a măsurilor tehnice și organizatorice de securitate.

Situațiile de excepție prevăzute de art. 30 alin. (5) din Regulamentul (UE) 2016/679 sunt de strictă interpretare.

(art. 30 din RGPD)

26. Când este necesară efectuarea evaluării de impact?

Evaluarea impactului asupra protecţiei datelor cu caracter personal de către operatori este obligatorie în special în următoarele cazuri:

1. prelucrarea datelor cu caracter personal efectuată în vederea realizării unei evaluări sistematice şi cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, şi care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;
2. prelucrarea pe scară largă a datelor cu caracter personal privind originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenenţa la sindicate, a datelor genetice, a datelor biometrice pentru identificarea unică a unei persoane fizice, a datelor privind sănătatea, viaţa sexuală sau orientarea sexuală ale unei persoane fizice sau a datelor cu caracter personal referitoare la condamnări penale şi infracţiuni;
3. prelucrarea datelor cu caracter personal având ca scop monitorizarea sistematică pe scară largă a unei zone accesibile publicului, cum ar fi supravegherea video în centre comerciale, stadioane, pieţe, parcuri sau alte asemenea spaţii;
4. prelucrarea pe scară largă a datelor cu caracter personal ale persoanelor vulnerabile, în special ale minorilor şi ale angajaţilor, prin mijloace automate de monitorizare şi/sau înregistrare sistematică a comportamentului, inclusiv în vederea desfăşurării activităţilor de reclamă, marketing şi publicitate;
5. prelucrarea pe scară largă a datelor cu caracter personal prin utilizarea

inovatoare sau implementarea unor tehnologii noi, în special în cazul în care operaţiunile respective limitează capacitatea persoanelor vizate de a-şi exercita drepturile, cum ar fi utilizarea tehnicilor de recunoaştere facială în vederea facilitării accesului în diferite spaţii;

6. prelucrarea pe scară largă a datelor generate de dispozitive cu senzori care transmit date prin internet sau prin alte mijloace (aplicaţii "Internetul lucrurilor", cum ar fi smart TV, vehicule conectate, contoare inteligente, jucării inteligente, oraşe inteligente sau alte asemenea aplicaţii);
7. prelucrarea pe scară largă şi/sau sistematică a datelor de trafic şi/sau de localizare a persoanelor fizice (cum ar fi monitorizarea prin Wi-Fi, prelucrarea datelor de localizare geografică a pasagerilor în transportul public sau alte asemenea situaţii) atunci când prelucrarea nu este necesară pentru prestarea unui serviciu solicitat de persoana vizată.

(Decizia președintelui autorității de supraveghere nr. 174/2018)

Pentru mai multe informații puteți accesa pe site-ul autorității de supraveghere www.dataprotection.ro:

- *Ghidul privind evaluarea de impact* emis de Comitetul European pentru Protecția Datelor, precum și
- *Decizia președintelui autorității de supraveghere nr. 174/2018 privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal.*

27. Ce trebuie să conțină evaluarea impactului asupra protecției datelor cu caracter personal?

Evaluarea trebuie să conțină cel puțin:

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

Pentru mai multe informații puteți accesa *Ghidul privind evaluarea de impact* emis de Comitetul European pentru Protecția Datelor, precum și *Ghidul*

orientativ de aplicare a Regulamentului general privind protecția datelor emis de Autoritatea Națională de Supraveghere.

28. Este necesară transmiterea în vederea avizării de către autoritatea de supraveghere a evaluării de impact realizată de operatorii de date cu caracter personal?

Operatorul consultă autoritatea de supraveghere înainte de prelucrare atunci când evaluarea impactului asupra protecţiei datelor indică faptul că prelucrarea ar genera un risc ridicat în absenţa unor măsuri luate de operator pentru atenuarea riscului.

Un astfel de risc este susceptibil să fie generat de anumite tipuri de prelucrare, precum și de amploarea și frecvența prelucrării, care pot duce și la producerea unor prejudicii sau pot atinge drepturile și libertățile persoanelor fizice.

Evaluarea de impact se prezintă la eventuala solicitare a Autorității Naționale de Supraveghere în cadrul efectuării unei investigații.

29. În ce moment ar trebui să fie efectuată o evaluare a impactului asupra protecției datelor cu caracter personal?

Evaluarea impactului asupra protecției datelor cu caracter personal trebuie să fie efectuată înaintea prelucrării.

Evaluarea impactului asupra protecției datelor cu caracter personal trebuie să înceapă cât mai curând posibil în elaborarea operațiunii de prelucrare, chiar dacă o parte din operațiunile de prelucrare încă nu sunt cunoscute.

Evaluarea impactului asupra protecției datelor cu caracter personal este un proces continuu, în special în cazul în care o operațiune de prelucrare este dinamică și în continuă schimbare.

Pentru mai multe informații puteți accesa *Ghidul privind evaluarea de impact* emis de Comitetul European pentru Protecția Datelor.

30. Ce înseamnă încălcarea securității datelor cu caracter personal?

Încălcarea securității datelor cu caracter personal înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea.

Încălcarea securității datelor cu caracter personal poate conduce la prejudicii de natură fizică, materială sau morală aduse persoanelor fizice, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau fraudă de identitate, pierdere financiară,

inversarea neautorizată a pseudonimizării, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional sau orice alt dezavantaj semnificativ de natură economică sau socială adus persoanei fizice în cauză.

Pentru mai multe informații se poate accesa *Ghidul privind notificarea încălcărilor de securitate* emis de Comitetul European pentru Protecția Datelor.

(art. 4 din RGPD)

31. În cât timp se notifică încălcările de securitate?

Cu excepţia cazului în care este puţin probabil ca o încălcare a securităţii datelor cu caracter personal să genereze un risc pentru drepturile şi libertăţile persoanelor fizice, operatorul are obligația de a notifica autorității de supraveghere orice încălcare a securităţii datelor, fără întârzieri nejustificate şi, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoştinţă de aceasta.

(art. 33 din RGPD)

32. Care este modalitatea de notificare a încălcării securității datelor cu caracter personal?

În cazul în care are loc o încălcare a securităţii datelor cu caracter personal, este necesar să se completeze on-line formularul adoptat prin Decizia nr. 128/2018 a președintelui Autorității de supraveghere pentru notificarea încălcării securităţii datelor cu caracter personal în conformitate cu Regulamentul (UE) 2016/679, existent pe site-ul autorității de supraveghere www.dataprotection.ro.

Formularul de notificare în format pdf, editabil, se completează de către operatori, se semnează digital și se transmite la adresa de e-mail a autorității de supraveghere, brese@dataprotection.ro. Formularele care nu vor fi semnate digital nu vor fi luate în considerare.

Operatorul trebuie să păstreze documente referitoare la toate cazurile de încălcare a securităţii datelor cu caracter personal, care să cuprindă o descriere a situaţiei de fapt în care a avut loc încălcarea securităţii datelor cu caracter personal, a efectelor acesteia şi a măsurilor de remediere întreprinse.

Informații în legătură cu modalitatea de notificare se regăsesc și pe site-ul Autorității de supraveghere, www.dataprotection.ro, la secţiunea „Notificare breşă GDPR", precum și în *Ghidul privind notificarea încălcărilor de securitate* emis de Comitetul European pentru Protecția Datelor.

33. Care sunt drepturile persoanei vizate?

La Capitolul III din Regulamentul (UE) 2016/679 sunt reglementate drepturile persoanei vizate:

- dreptul la informare (art. 13 și art. 14);
- dreptul de acces (art. 15);
- dreptul la rectificare (art. 16);
- dreptul la ștergere („dreptul de a fi uitat" – art. 17);
- dreptul la restricționarea prelucrării (art. 18);
- dreptul la portabilitatea datelor (art. 20);
- dreptul la opoziție (art. 21);
- dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată (art. 22);
- dreptul de a depune o plângere la o autoritate de supraveghere (art. 77).

Pentru exercitarea drepturilor prevăzute la art. 15 – 22 din Regulamentul (UE) 2016/679, este necesar ca persoanele vizate să adreseze o cerere operatorului în acest sens.

Pentru mai multe informații puteți accesa *Ghidul privind dreptul la portabilitatea datelor, Ghidul privind deciziile automate individuale și profilare, Ghidul privind transparența,* emise de Comitetul European pentru Protecția Datelor.

34. În ce termen trebuie să răspundă operatorul la o cerere de exercitare a drepturilor persoanei vizate?

Operatorul furnizează persoanei vizate informaţii privind acţiunile întreprinse în urma unei cereri în temeiul articolelor 15-22 din Regulament în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu două luni atunci când este necesar, ţinându-se seama de complexitatea şi numărul cererilor.

Operatorul informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând şi motivele întârzierii.

(art. 12 din RGPD)

35. Ce informații trebuie să furnizeze operatorul persoanei vizate?

Operatorul furnizează persoanei vizate, atunci când obține datele direct sau indirect de la aceasta, următoarele informaţii:

1. identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acestuia;
2. datele de contact ale responsabilului cu protecţia datelor, după caz;

3. scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării;
4. categoriile de date cu caracter personal vizate (în cazul datelor obținute indirect)
5. interesele legitime urmărite de operator sau de o parte terţă (dacă este cazul);
6. destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
7. intenţia operatorului de a transfera date cu caracter personal către o ţară terţă sau o organizaţie internaţională și condițiile în care se realizează transferul (dacă este cazul).
8. perioada de stocare a datelor cu caracter personal (sau criterii pentru stabilirea perioadei);
9. existenţa drepturilor persoanei vizate prevăzute de Regulament;
10. existenţa dreptului de a-și retrage consimţământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia;
11. dreptul de a depune o plângere în faţa unei autorităţi de supraveghere;
12. dacă furnizarea de date cu caracter personal reprezintă o obligaţie legală sau contractuală sau o obligaţie necesară pentru încheierea unui contract, precum şi dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal şi care sunt eventualele consecinţe ale nerespectării acestei obligaţii;
13. existenţa unui proces decizional automatizat incluzând crearea de profiluri, informații privind logica utilizată și consecințele prelucrării asupra persoanei vizate;
14. prelucrarea datelor într-un alt scop decât cel pentru care acestea au fost colectate (dacă este cazul);
15. sursa din care provin datele cu caracter personal și dacă acestea provin din surse disponibile public (în cazul datelor obținute indirect).

(art. 13 și 14 din RGPD)

36. Când trebuie realizată informarea persoanelor vizate în situația în care datele cu caracter personal nu au fost obţinute de la acestea?

În cazul în care datele cu caracter personal nu au fost obţinute de la persoana vizată, operatorul informează persoana vizată:

1. într-un termen rezonabil după obţinerea datelor cu caracter personal, dar nu mai mare de o lună, ţinându-se seama de circumstanţele specifice în care sunt prelucrate datele cu caracter personal;
2. cel târziu în momentul primei comunicări către persoana vizată respectivă, dacă datele cu caracter personal urmează să fie utilizate pentru

comunicarea cu persoana vizată,; sau

3. cel mai târziu la data la care acestea sunt divulgate pentru prima oară, dacă se intenţionează divulgarea datelor cu caracter personal către un alt destinatar.

În ceea ce privește modalitatea prin care se realizează informarea persoanelor vizate (indiferent de temeiul prelucrării, la consimțământ sau pe bază de excepții) operatorul trebuie să ia măsuri adecvate, în funcție de circumstanțele prelucrării datelor, pentru a furniza persoanei vizate informaţiile menţionate de RGPD, într-o formă **concisă, transparentă, inteligibilă şi uşor accesibilă**, utilizând un **limbaj clar şi simplu**.

Informaţiile se furnizează **în scris sau prin alte mijloace,** inclusiv, atunci când este oportun, în **format electronic.**

Pentru informare se poate apela la o informare generică, expusă pe site-ul operatorului, afișare la avizier la sediul operatorului, la note de informare directă a persoanei vizate, concomitent cu furnizarea de broșuri și pliante, precum și la alte modalități ce sunt stabilite de operator.

Pentru mai multe informații puteți accesa *Ghidul privind transparența,* emis de Comitetul European pentru Protecția Datelor.

(art. 14 din RGPD)

37. Poate avea acces persoana vizată la datele sale personale prelucrate de operator?

Persoana vizată are dreptul de a obține din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc. În cazul în care răspunsul operatorului este afirmativ, persoana vizată are dreptul de a cunoaște și de a i se comunica următoarele informații:

- scopurile prelucrării;
- categoriile de date cu caracter personal vizate;
- destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate;
- perioada de stocare a datelor cu caracter personal sau criteriile utilizate pentru a stabili această perioadă;
- existența dreptului de a solicita operatorului rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării;
- dreptul de a depune o plângere în fața unei autorități de supraveghere;
- orice informații disponibile privind sursa acestora (în cazul datelor obținute indirect);
- existența unui proces decizional automatizat incluzând crearea de

profiluri, informații privind logica utilizată și consecințele prelucrării asupra persoanei vizate;
- transferul către o țară terță sau o organizație internațională și garanțiile adecvate referitoare la transfer.

Operatorul furnizează persoanei vizate o copie a datelor cu caracter personal care fac obiectul prelucrării. Pentru orice alte copii solicitate de persoana vizată, operatorul poate percepe o taxă rezonabilă, bazată pe costurile administrative.

Dacă persoana vizată transmite cererea în format electronic și nu optează să primească informațiile în alt format, acestea se furnizează într-un format electronic utilizat în mod curent.

Pentru mai multe informații puteți accesa *Ghidul privind transparența,* emis de Comitetul European pentru Protecția Datelor.

(art. 15 din RGPD)

38. Care sunt situațiile în care persoana vizată poate obține ștergerea datelor cu caracter personal din partea operatorului („dreptul de a fi uitat")?

Persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, în următoarele situații:
- datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;
- 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 potrivit condițiilor exercitării dreptului la opoziție;
- datele cu caracter personal au fost prelucrate ilegal;
- datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale care revine operatorului;
- datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societății informaționale unui copil.

Dacă operatorul a făcut publice datele și este obligat să le șteargă, trebuie să ia măsuri rezonabile (inclusiv tehnice), ținând seama de tehnologia disponibilă și de costul implementării, pentru a informa ceilalți operatori că persoana vizată a solicitat ștergerea de către acești operatori a oricăror linkuri către datele respective sau a oricăror copii sau reproduceri ale datelor în cauză.

(art. 17 din RGPD)

39. Care sunt condițiile de exercitare a dreptului la opoziție?

Persoanele vizate au dreptul de a se opune prelucrării oricăror date cu caracter personal care le privesc, din motive legate de situația particulară în care se află, atunci când datele sunt prelucrate pentru:

- îndeplinirea unei sarcini care servește unui interes public
- îndeplinirea unei sarcini care rezultă din exercitarea autorității publice cu care este învestit operatorul
- scopul intereselor legitime ale unui operator sau ale unei părți terțe.
- scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, cu excepţia cazului în care prelucrarea este necesară pentru îndeplinirea unei sarcini din motive de interes public.

Operatorul nu mai prelucrează datele cu caracter personal, cu excepţia cazului în care demonstrează că are motive legitime şi imperioase care justifică prelucrarea şi care prevalează asupra intereselor, drepturilor şi libertăţilor persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanţă.

În cazul în care datele cu caracter personal sunt prelucrate în scopuri de marketing direct, persoana vizată are dreptul de a se opune unei astfel de prelucrări, inclusiv creării de profiluri în măsura în care aceasta are legătură cu marketingul direct, în orice moment și în mod gratuit. În acest caz, operatorul nu mai prelucrează datele cu caracter personal.

Cel târziu în momentul primei comunicări cu persoana vizată, dreptul la opoziție este adus în mod **explicit** în atenţia persoanei vizate şi este prezentat **în mod clar şi separat** de orice alte informaţii.

(art. 21 din RGPD)

40. Care sunt situațiile în care persoana vizată nu poate obține ștergerea datelor cu caracter personal din partea operatorului?

Persoana vizată nu poate obține ștergerea datelor cu caracter personal din partea operatorului în măsura în care prelucrarea este necesară:

- pentru exercitarea dreptului la liberă exprimare şi la informare;
- pentru respectarea unei obligaţii legale;
- din motive de interes public în domeniul sănătăţii publice;
- în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice (dreptul se poate exercita dacă ștergerea nu face imposibilă sau nu afectează în mod grav realizarea obiectivelor prelucrarii respective);
- pentru constatarea, exercitarea sau apărarea unui drept în instanţă.

(art. 17 din RGPD)

41. Care sunt condițiile în care persoana vizată poate transmite datele sale altui operator (dreptul la portabilitatea datelor)?

Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc și pe care le-a furnizat operatorului într-un format structurat și are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal, în cazul în care:

- prelucrarea se bazează pe **consimțământ** și
- prelucrarea este efectuată prin **mijloace automate**
- Persoana vizată are dreptul ca datele să fie transmise și în mod direct de la un operator la altul, dacă este fezabil din punct de vedere tehnic.
- Acest drept nu aduce atingere dreptului de a obține ștergerea datelor și nu poate afecta drepturile și libertățile altora.

(art. 20 din RGPD)

42. În ce situații poate face persoana vizată obiectul unei decizii bazate pe prelucrarea automată, inclusiv crearea de profiluri?

Regula este aceea că persoana vizată are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă.

Cu toate acestea, persoana vizată poate face obiectul unei decizii bazate pe prelucrarea automată, inclusiv crearea de profiluri, în cazul în care decizia:

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

În aceste din urmă două cazuri operatorul de date pune în aplicare măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate, privind cel puţin:

- dreptul acesteia de a obţine intervenţie umană din partea operatorului,
- de a-şi exprima punctul de vedere şi
- de a contesta decizia.

Decizia nu are la bază categoriile speciale de date cu caracter personal, cu excepţia cazului în care se prelucrează datele pe baza consimţământului sau în interes public major şi au fost instituite măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate.

(art. 22 din RGPD)

43. Cum se realizează transferul de date într-o ţară terţă sau către o organizaţie internaţională?

Principiul de bază al transferurilor este acela că orice date cu caracter personal pot fi transferate doar dacă condiţiile prevăzute în Regulament sunt respectate atât de operator, cât şi de împuternicit, inclusiv în ceea ce priveşte transferurile ulterioare în alte state terţe.

Transferul de date cu caracter personal se poate realiza în baza unor:
decizii ale Comisiei europene privind caracterul adecvat al nivelului de protecţie asigurat de statul terţ;

- clauze standard de protecţie a datelor adoptate de Comisia europeană;
- reguli corporatiste obligatorii (BCR) în conformitate cu art. 47 din Regulament
- alte modalităţi prevăzute la art. 46 şi art. 49 din Regulament, precum:
- un instrument obligatoriu din punct de vedere juridic şi executoriu între autorităţile sau organismele publice
- clauze standard de protecţie a datelor adoptate de autoritatea de supraveghere şi aprobate de Comisia europeană
- cod de conduită aprobat şi însoţit de un angajament de respectare din partea operatorului sau împuternicitului din ţara terţă
- un mecanism de certificare aprobat şi însoţit de un angajament de respectare din partea operatorului sau împuternicitului din ţara terţă
- clauze contractuale între operator sau persoana împuternicită de operator şi operatorul, persoana împuternicită de operator sau destinatarul datelor cu caracter personal din ţara terţă sau organizaţia internaţională; sau
- dispoziţii care urmează să fie incluse în acordurile administrative dintre autorităţile sau organismele publice, care includ drepturi opozabile şi efective pentru persoanele vizate.

Derogări pentru situaţii specifice (art. 49 din RGPR)

În absenţa unei decizii privind caracterul adecvat al nivelului de protecţie sau a unor garanţii adecvate transferurile pot avea loc numai în una dintre situaţiile următoare:

- Acordul explicit al persoanei vizate - informare prealabilă

- Executarea unui contract între persoana vizată şi operator (măsuri precontract.)
- Încheierea/Executarea unui contract încheiat în interesul persoanei vizate
- Interesul public
- Stabilirea, exercitarea sau apărarea unui drept în instanţă
- Protejarea intereselor vitale ale persoanei vizate sau ale altor persoane
- Furnizarea de informaţii dintr-un registru accesibil publicului
- Alte situații, în anumite condiții, cu prezentarea de către oeprator a unor garanții corespunzătoare

Pentru mai multe informații puteți accesa următoarele documente, disponibile pe site-ul autorității de supraveghere www.dataprotection.ro:

- *Ghidul privind derogările aplicabile transferurilor internaționale (art. 49 din Regulamentul General privind Protecția Datelor),* emis de Comitetul European pentru Protecția Datelor*;*
- *Recomandarea privind cererea standard de aprobare a regulilor corporatiste obligatorii pentru transferul datelor cu caracter personal, aplicabile operatorilor (WP 264);*
- *Documentul de lucru Stabilirea unei proceduri de cooperare pentru aprobarea "Regulilor corporatiste obligatorii" pentru operatori și împuterniciți, conform GDPR (WP 263);*
- *Documentul de lucru care stabilește un tabel cu elementele și principiile care se regăsesc în Regulile corporatiste obligatorii (WP 256);*
- *Document de lucru care stabilește un tabel cu elementele și principiile care trebuie găsite în Regulile corporatiste obligatorii, aplicabile împuterniciților (WP 257);*
- *Recomandarea privind formularul standard de solicitare a aprobării regulilor corporatiste obligatorii pentru transferul datelor cu caracter personal, aplicabile împuterniciților (WP 265).*

44. Care sunt situațiile în care autoritatea de supraveghere emite autorizații pentru transferul datelor cu caracter personal?

În situația în care transferul nu poate fi efectuat în baza unei decizii privind caracterul adecvat al nivelului de protecție, operatorul sau persoana împuternicită de operator poate transfera date cu caracter personal către o ţară terţă sau o organizaţie internaţională, sub rezerva autorizării din partea autorității de supraveghere, prin:

- clauze contractuale între operator sau persoana împuternicită de operator și operatorul, persoana împuternicită de operator sau destinatarul datelor cu caracter personal din țara terță sau organizația internațională; sau

- dispoziții care urmează să fie incluse în acordurile administrative dintre autoritățile sau organismele publice, care includ drepturi opozabile și efective pentru persoanele vizate.
- Pentru mai multe informații puteți accesa Opinia 04/2019 privind acordurile administrative pentru transferul datelor cu caracter personal între autoritățile de supraveghere financiară din Spațiul Economic European ("SEE") și autoritățile de supraveghere financiară din afara SEE.

(art. 46 alin. (3) din RGPD)

45. Deciziile adoptate de Comisia Europeană în temeiul art. 26 alin. 4 din Directiva 95/46/CE mai sunt valabile după aplicarea Regulamentului (UE) 2016/679?

Deciziile adoptate de Comisia Europeană în temeiul art. 26 alin. 4 din Directiva 95/46/CE **rămân în vigoare până când sunt modificate, înlocuite sau abrogate de o decizie a Comisiei** adoptată în conformitate cu alin. (2) din art. 46 din Regulamentul (UE) 2016/679.

Ca atare, sunt aplicabile următoarele decizii:

- Decizia 2010/87/UE din 5 februarie 2010 privind clauzele contractuale tip pentru transferul de date cu caracter personal către persoanele împuternicite de către operator stabilite în țări terțe în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului;
- Decizia 2004/915/CE din 27 decembrie 2004 de modificare a Deciziei 2001/497/CE privind introducerea unui set alternativ de clauze contractuale standard pentru transferul de date cu caracter personal către țări terțe;
- Decizia 2001/497/CE din 15 iunie 2001 privind clauzele contractuale standard pentru transferul de date cu caracter personal către țările terțe în temeiul Directivei 95/46/CE.

46. Ce măsuri trebuie să ia operatorii și persoanele împuternicite de operatori pentru asigurarea securității prelucrării datelor cu caracter personal?

În vederea asigurării unui nivel de securitate corespunzător, operatorii și persoanele împuternicite de operatori trebuie să implementeze măsuri tehnice și organizatorice adecvate, cum ar fi:

- 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 a eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.
- pseudonimizarea și criptarea datelor cu caracter personal, după caz (aplicarea pseudonimizării datelor cu caracter personal poate reduce riscurile pentru persoanele vizate si poate ajuta operatorii și persoanele imputernicite de aceştia să își îndeplinească obligațiile de protecție a datelor).
- asigurarea faptului că orice persoană fizică care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator şi care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care această obligație îi revine în temeiul dreptului Uniunii sau al dreptului intern.

Aderarea la un cod de conduită aprobat sau la un mecanism de certificare aprobat poate fi utilizată ca element prin care să se demonstreze de către operator sau împuternicit îndeplinirea cerinţelor privind implementarea de măsuri tehnice și organizatorice adecvate.

(art. 32 din RGPD)

47. Ce înseamnă „pseudonimizare"?

Pseudonimizarea este definită ca fiind prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anumite persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane.

(art. 4 din RGPD)

48. Cât timp pot stoca datele cu caracter personal?

Datele cu caracter personal trebuie păstrate într-o formă care să permită identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele.

Datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, cu instituirea unor garanții.

Astfel, operatorului i se conferă posibilitatea de a avea diferite termene de stocare a datelor, în funcție de scopul/scopurile prelucrării și pe durata

necesară realizării lor, fie prin stabilirea din proprie inițiativă a unei durate maxime de păstrare, cu respectarea principiului proporționalității, fie prin respectarea unor termene prevăzute în diferite acte normative specifice.

Dacă perioada de stocare este stabilită prin acte normative ce reglementează domenii specifice de activitate, în măsura în care se impune, entitățile abilitate trtebuie să procedeze la modificarea/completarea acestora astfel încât normele să fie puse în conformitate cu Regulamentul general privind protecția datelor.

(art. 5 din RGPD)

49. Asociațiile de proprietari pot prelucra datele cu caracter personal ale proprietarilor/locatarilor prin utilizarea mijloacelor de supraveghere video în baza interesului legitim?

Prelucrarea datelor cu caracter personal prin utilizarea unor sisteme **de televiziune cu circuit închis** cu posibilităţi de înregistrare şi stocare a imaginilor şi datelor se supune atât prevederilor **Regulamentului** general privind protecția datelor, cât şi ale **Legii nr. 333/2003** privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor, modificată şi completată și a Normelor metodologice de aplicare a acestei legi.

În contextul în care instalarea unui sistem de supraveghere video este necesară în vederea realizării unui interes legitim al asociaţiei de proprietari (asigurarea pazei şi protecției persoanelor, bunurilor și valorilor, a imobilelor și a instalațiilor de utilitate publică, precum și a împrejmuirilor afectate acestora), hotărârea de a instala un astfel de sistem trebuie adoptată în cadrul adunării generale a asociaţiei de proprietari.

Potrivit art. 48 alin. (1) din **Legea nr. 196/2018 privind înfiinţarea, organizarea şi funcţionarea asociaţiilor de proprietari şi administrarea condominiilor**, "Adunarea generală poate adopta hotărâri, dacă majoritatea proprietarilor membri ai asociației de proprietari sunt prezenți personal sau prin reprezentanți care au o împuternicire scrisă și semnată de către proprietarii în numele cărora votează". De asemenea, la alin. (3) al aceluiași articol se precizează că hotărârile adunării generale a asociației de proprietari pot fi adoptate prin votul majorităţii acestora.

În plus, trebuie să se ţină cont şi de interesele, drepturile şi libertăţile persoanelor vizate. Acestea trebuie informate anterior cu privire la luarea unei astfel de măsuri. În acest sens, în spaţiile monitorizate trebuie instalată o pictogramă adecvată, care să conţină o imagine reprezentativă, poziţionată la o distanţă rezonabilă de locurile unde sunt amplasate echipamentele de supraveghere, astfel încât să poată fi văzută de orice persoană.

Autoritatea Națională de Supraveghere recomandă ca perioada de stocare

a datelor cu caracter personal (imagini) prelucrate de asociaţie ca urmare a instalării sistemului de supraveghere video să nu depăşească 30 zile.

Excepție pot face situațiile temeinic justificate în care s-au produs evenimente ce necesită stocarea doar a imaginilor relevante pe o perioadă mai mare de timp necesară îndeplinirii scopurilor respective (de ex. până la soluționarea definitivă a unei cauze penale de către organele judiciare).

50. În ce condiții pot fi publicate listele de plată de către asociațiile de proprietari?

Potrivit art. 6 din Regulamentul (UE) 2016/679 prelucrarea este legală numai în masura în care se aplică cel puțin una din condițiile prevăzute la alin. (1) al aceluiași articol.

Regulamentul (UE) 2016/679 introduce în art. 5 un nou principiu de prelucrare a datelor, cel al responsabilității, potrivit căruia operatorii de date cu caracter personal nu numai că sunt responsabili de respectarea tuturor principiilor de prelucrarea a datelor (”legalitate, echitate şi transparenţă”, "limitări legate de scop", "reducerea la minimum a datelor", "exactitate", ”limitări legate de stocare", precum și "integritate şi confidenţialitate"), dar este necesar ca aceștia să poată demonstra respectarea principiilor menționate.

Potrivit art. 5 din Regulament datele cu caracter personal sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate.

Prelucrarea datelor proprietarilor în contextul publicării listelor de plată se poate realiza cu consimțământul acestora în baza prevederilor art. 6 alin. (1) lit. a) din Regulament, cu respectarea principiilor și regulilor de protecție a datelor stabilite de acest act normativ.

51. Instituțiile publice pot publica pe site-ul propriu datele cu caracter personal ale persoanelor care participă la concursuri pentru ocuparea unor posturi corespunzătoare funcțiilor contractuale?

Potrivit art. 6 din Regulamentul (UE) 2016/679 prelucrarea este legală numai în masura în care se aplică cel puțin una din condițiile prevăzute la alin. (1) al aceluiași articol, unele dintre acestea fiind consimțământul persoanei vizate sau îndeplinirea unei obligații legale.

Prin urmare, dacă dispozițiile legale în materie nu prevăd în mod expres ca obligație legală publicarea pe site-ul autorităților publice a numelui și prenumelui candidaților, aceasta se poate realiza numai cu consimțământul cadidaților, în baza prevederilor art. 6 alin. (1) lit. a) din Regulament, cu respectarea principiilor și regulilor de protecție a datelor stabilite de acest act normativ.

52. Cine poate elabora coduri de conduită?

Potrivit dispozițiilor art. 40 alin. (2) din Regulamentul (UE) 2016/679, asociaţiile şi alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori pot pregăti coduri de conduită sau le pot modifica sau extinde pe cele existente, în scopul de a specifica modul de aplicare a Regulamentului.

Pentru mai multe informații puteți accesa *Ghidul nr. 1/2019 privind Codurile de conduită și organismele de monitorizare în temeiul Regulamentului 2016/679* emis de Comitetul European pentru Protecția Datelor.

53. Codurile de conduită se transmit spre avizare și aprobare autorității de supraveghere?

Asociaţiile şi alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori care intenţionează să pregătească un cod de conduită sau să modifice sau să extindă un cod existent, transmit proiectul de cod, de modificare sau de extindere, autorității de supraveghere. Autoritatea de supraveghere emite un aviz cu privire la conformitatea cu Regulamentul a proiectului de cod, de modificare sau de extindere şi îl aprobă în cazul în care se constată că acesta oferă garanţii adecvate suficiente.

Pentru mai multe informații puteți accesa *Ghidul nr. 1/2019 privind Codurile de conduită și organismele de monitorizare în temeiul Regulamentului 2016/679* emis de Comitetul European pentru Protecția Datelor.
(art. 40 din RGPD)

54. Ce ghiduri a emis Comitetul European pentru protecția datelor?

- Comitetul european pentru protecția datelor a adoptat și dat publicității, o serie de ghiduri, orientări și opinii utile celor interesați, astfel:
- *Ghidul privind responsabilul pentru protecția datelor;*
- *Ghidul privind consimțământul;*
- *Ghidul privind dreptul la portabilitatea datelor;*
- *Ghidul privind transparența;*
- *Ghidul privind evaluarea de impact;*
- *Ghidul privind stabilirea autorității de supraveghere principale a operatorului sau a persoanei împuternicite de operator;*
- *Ghidul privind notificarea încălcărilor de securitate;*
- *Ghidul privind deciziile automate individuale și profilare;*
- *Orientări privind derogările prevăzute la art. 49 din Regulamentul (UE) 2016/679;*
- *Ghidul nr. 4/2018 privind acreditarea organismelor de certificare în temeiul articolului 43 din Regulamentul general privind protecția datelor (2016/679);*

- *Ghidul nr. 1/2018 privind certificarea și identificarea criteriilor de certificare în conformitate cu articolele 42 și 43 din Regulamentul general privind protecția datelor (2016/679);*
- *Ghidul nr. 2/2018 privind derogările prevăzute la articolul 49 din Regulamentul (UE) 2016/679;*
- *Ghidul privind aplicarea și stabilirea amenzilor administrative în sensul Regulamentului 2016/679;*
- *Ghidul nr. 1/2019 privind Codurile de conduită și organismele de monitorizare în temeiul Regulamentului 2016/679*
- *Documentul de poziție privind derogările de la obligația de a păstra o evidență a activităților de prelucrare în conformitate cu art. 30 (5) din Regulamentul (UE) 2016/679;*
- *Opinia 04/2019 privind acordurile administrative pentru transferul datelor cu caracter personal între autoritățile de supraveghere financiară din Spațiul Economic European ("SEE") și autoritățile de supraveghere financiară din afara SEE.*

Aceste ghiduri pot fi găsite pe adresa de internet a autorității, www.dataprotection.ro, la secțiunea dedicată Regulamentului General de Protecția Datelor, precum și pe adresa de internet a Comitetului Europen pentru Protecția Datelor www.edpb.europa.eu.

55. Ce ghiduri a emis Autoritatea Națională de supraveghere?

Autoritatea Națională de Supraveghere a pus la dispoziția publicului, pe site-ul său:

- *Ghidul orientativ de aplicare a Regulamentului general privind protecția datelor* și
- *Ghidul privind întrebări și răspunsuri cu privire la aplicarea Regulamentului (UE) 2016/679,* acestea fiind accesibile la secțiunea dedicată Regulamentului General de Protecția Datelor.

56. Care sunt elementele de noutate aduse de Legea nr. 190/2018?

Legea nr. 190/2018 aduce următoarele elemente de noutate:

- **menționează expres autoritățile și organismele publice** cărora le sunt aplicabile dispozițiile Regulamentului General privind Protecția Datelor;
- **definește o serie de termeni** cum ar fi: număr de identificare național, plan de remediere, măsură de remediere, termen de remediere (art. 2);
- **stabilește reguli speciale privind prelucrarea unor categorii de date cu caracter personal**, precum date genetice, date biometrice sau date privind sănătatea (art. 3);
- **stabilește condițiile de prelucrare a unui număr de identificare**

naţional (de exemplu, codul numeric personal) atunci când prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță (art. 4);

- **instituie prevederi specifice privind prelucrarea datelor cu caracter personal în contextul relaţiilor de muncă** (art. 5);
- **prevede derogări** pentru prelucrările efectuate în scopuri jurnalistice, al exprimării academice, artistice sau literare ori în scopuri de cercetare ştiinţifică, istorică, statistică, de arhivare în interes public (art. 7 și art. 8);
- **menționează condițiile desemnării și sarcinile responsabilului cu protecţia datelor**, în special în cazul autorităților/instituțiilor publice și a organismelor publice (art. 10);
- **desemnează Asociația de Acreditare din România – RENAR** ca organism național de acreditare a organismelor de certificare prevăzute la art. 43 din Regulament;
- stabilește regimul sancționator derogatoriu, inclusiv sub aspectul sancțiunilor pecuniare, aplicabil autorităților și organismelor publice, acordându-se prioritate mecanismului de prevenire, anterior aplicării amenzilor contravenționale (art. 12, art. 13 și art. 14).

57. Ce înseamnă autorități și organisme publice?

Autoritățile și organismele publice sunt: Camera Deputaților și Senatul, Administrația Prezidențială, Guvernul, ministerele, celelalte organe de specialitate ale administrației publice centrale, autoritățile și instituțiile publice autonome, autoritățile administrației publice locale și deja nivel județean, alte autorități publice, precum și instituțiile din subordinea/coordonarea acestora; de asemenea, sunt asimilate autorităților/organismelor publice și unitățile de cult și asociațiile și fundațiile de utilitate publică potrivit art. 2 alin. (1) lit. a din Legea nr. 190/2018.

În măsura în care entitatea în cauză, potrivit actelor normative de înființare, organizare și funcționare, se înscrie stricto-sensu în definiția dată de textul de lege, dispozițiile specifice din Legea nr. 190/2018, inclusiv sub aspectul sancțiunilor, devin aplicabile.

58. În ce condiții se poate realiza prelucrarea datelor genetice, a datelor biometrice sau a datelor privind sănătatea în scopul realizării unui proces decizional automatizat sau pentru crearea de profiluri?

Prelucrarea acestor categorii de date speciale, în scopul realizării unui proces decizional automatizat sau pentru crearea de profiluri, **este permisă cu consimţământul explicit** al persoanei vizate sau dacă prelucrarea este efectuată în temeiul unor dispoziţii legale exprese, cu instituirea unor măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime

ale persoanei vizate.

(art. 3 din Legea nr. 190/2018)

59. Ce înseamnă număr de identificare național?

Numărul de identificare naţional reprezintă numărul prin care se identifică o persoană fizică în anumite sisteme de evidenţă şi care are aplicabilitate generală, cum ar fi: codul numeric personal, seria şi numărul actului de identitate, numărul paşaportului, al permisului de conducere, numărul de asigurare socială de sănătate.

(art. 2 din Legea nr. 190/2018)

60. În ce condiții se poate realiza prelucrarea datelor în temeiul interesului legitim, inclusiv a unui număr de identificare naţional?

Prelucrarea unui număr de identificare naţional, inclusiv prin colectarea sau dezvăluirea documentelor ce îl conţin se poate efectua în situaţiile prevăzute de art. 6 alin. (1) din Regulamentul general privind protecţia datelor.

În situația în care prelucrarea unui număr de identificare naţional este necesară în scopul realizării intereselor legitime urmărite de operator sau de o parte terţă, aceasta se efectuează cu instituirea de către operator a următoarelor garanţii:

- punerea în aplicare de măsuri tehnice şi organizatorice adecvate pentru respectarea, în special, a principiului reducerii la minimum a datelor, precum şi pentru asigurarea securităţii şi confidenţialităţii prelucrărilor de date cu caracter personal, conform dispoziţiilor art. 32 din Regulamentul general privind protecţia datelor;
- numirea unui responsabil pentru protecţia datelor, potrivit art. 10 din lege și în conformitate cu prevederile art. 37-39 din Regulament;
- stabilirea de termene de stocare în funcţie de natura datelor şi scopul prelucrării, precum şi de termene specifice în care datele cu caracter personal trebuie şterse sau revizuite în vederea ştergerii;
- instruirea periodică cu privire la obligaţiile ce le revin persoanelor care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, prelucrează date cu caracter personal.

În consecință, în măsura în care se invocă interesul legitim al operatorului, acesta se impune a fi temeinic justificat, astfel încât să prevaleze asupra intereselor, drepturilor și libertăților fundamentale ale persoanelor fizice în cauză, cu atât mai mult cu cât datele urmează a fi prelucrate fără consimțământul persoanelor vizate. Justificarea trebuie să se regăsească într-o documentație păstrată de operator.

Autoritatea Națională de Supraveghere poate fi consultată sub acest aspect de operator sau de persoana împuternicită de operator.

(art. 4 din Legea nr. 190/2018)

61. În ce condiții pot fi prelucrate datele agajaților la locul de muncă în situația în care sunt utilizate sisteme de monitorizare prin mijloace de comunicații electronice și/sau prin mijloace de supraveghere video?

Întrucât sistemele de monitorizare prin mijloace de comunicații electronice și/sau prin mijloace de supraveghere video comportă anumite riscuri în privinţa drepturilor şi libertăţilor persoanei, înainte de instalarea unor astfel de sisteme de supraveghere, angajatorul trebuie să facă în prealabil o evaluare a riscurilor la care se supune activitatea sa pentru a stabili necesitatea implementării lor.

În conformitate cu prevederile *art. 5 din Legea nr. 190/2018*, prelucrarea datele agajaților la locul de muncă prin utilizarea sistemelor de monitorizare prin mijloace de comunicații electronice și/sau prin mijloace de supraveghere video, în scopul realizării intereselor legitime urmărite de operator, este permisă numai dacă:

a) interesele legitime urmărite de angajator sunt temeinic justificate şi prevalează asupra intereselor sau drepturilor şi libertăţilor persoanelor vizate;

b) angajatorul a realizat informarea prealabilă obligatorie, completă şi în mod explicit a angajaţilor;

c) angajatorul a consultat sindicatul sau, după caz, reprezentanţii angajaţilor înainte de introducerea sistemelor de monitorizare;

d) alte forme şi modalităţi mai puţin intruzive pentru atingerea scopului urmărit de angajator nu şi-au dovedit anterior eficienţa; şi

e) durata de stocare a datelor cu caracter personal este proporţională cu scopul prelucrării, dar nu mai mare de 30 de zile, cu excepţia situaţiilor expres reglementate de lege sau a cazurilor temeinic justificate.

În această privință poate fi consultată Autoritatea Națională de Supraveghere.

Aceste aspecte trebuie să se regăsească la angajator într-o documentație argumentată temeinic, din care să rezulte prevalența interesului legitim asupra intereselor sau drepturilor şi libertăţilor angajaților.

Pentru mai multe informații puteți consulta Avizul 06/2014 privind noțiunea de interese legitime ale operatorului de date (WP 217) emis de Grupul de Lucru Art. 29 (în prezent Comitetul european pentru protecția datelor).

(art. 5 din Legea nr. 190/2018)

62. În ce condiții pot fi prelucrate datele cu caracter personal, în contextul îndeplinirii unei sarcini care serveşte unui interes public?

În contextul îndeplinirii unei **sarcini care serveşte unui interes public**, prelucrarea datelor cu caracter personal se realizează cu instituirea de către operator sau de către partea terţă a următoarelor garanţii:

- *punerea în aplicare a măsurilor tehnice şi organizatorice adecvate, în special a reducerii la minimum a datelor, respectiv a principiului integrităţii şi confidenţialităţii;*
- *numirea unui responsabil pentru protecţia datelor (dacă este cazul, potrivit legii);*
- *stabilirea de termene de stocare în funcţie de natura datelor şi scopul prelucrării, precum şi de termene specifice în care datele cu caracter personal trebuie şterse sau revizuite în vederea ştergerii.*

(art. 6 din Legea nr. 190/2018)

63. În ce condiții pot fi prelucrate datele cu caracter personal în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare?

Prelucrarea în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare poate fi efectuată, dacă aceasta priveşte date cu caracter personal care au fost făcute publice în mod manifest de către persoana vizată sau care sunt strâns legate de calitatea de persoană publică a persoanei vizate ori de caracterul public al faptelor în care este implicată, prin derogare de la următoarele capitole din Regulamentul general privind protecţia datelor:

a) capitolul II - Principii;
b) capitolul III - Drepturile persoanei vizate;
c) capitolul IV - Operatorul şi persoana împuternicită de operator;
d) capitolul V - Transferurile de date cu caracter personal către ţări terţe sau organizaţii internaţionale;
e) capitolul VI - Autorităţi de supraveghere independente;
f) capitolul VII - Cooperare şi coerenţă;
g) capitolul IX - Dispoziţii referitoare la situaţii specifice de prelucrare.

(art. 7 din Legea nr. 190/2018)

64. Persoanele vizate își pot exercita drepturile prevăzute în Regulamentul (UE) 2016/679 în cazul prelucrării datelor acestora în scopuri de cercetare ştiinţifică sau istorică?

Prevederile art. 15 (**dreptul de acces** al persoanei vizate), art. 16 (**dreptul la rectificarea datelor**), art. 18 (**dreptul la restricționarea prelucrării**) şi art. 21 (**dreptul la opoziție**) din Regulamentul general privind protecţia datelor **nu se aplică** în cazul în care datele cu caracter personal pot fi prelucrate în scopuri de cercetare ştiinţifică sau istorică.

Derogările de mai sus se aplică în măsura în care drepturile menţionate la aceste articole sunt de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice și sub rezerva existenţei garanţiilor corespunzătoare pentru drepturile şi libertăţile persoanelor vizate.

(art. 8 din Legea nr. 190/2018)

65. Persoanele vizate își pot exercita drepturile prevăzute în Regulamentul (UE) 2016/679 în cazul prelucrării datelor acestora în scopuri statistice ori în scopuri de arhivare în interes public?

Prevederile art. 15 (**dreptul de acces** al persoanei vizate), art. 16 (**dreptul la rectificarea datelor**), art. 18 (**dreptul la restricționarea prelucrării**), art. 20 (**dreptul la portabilitatea datelor**) şi art. 21 (**dreptul la opoziție**) din Regulamentul general privind protecţia datelor **nu se aplică** în cazul în care datele cu caracter personal sunt prelucrate în scopuri de arhivare în interes public.

Derogările de mai sus se aplică în măsura în care drepturile menţionate la aceste articole sunt de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice și sub rezerva existenţei garanţiilor corespunzătoare pentru drepturile şi libertăţile persoanelor vizate.

(art. 8 din Legea nr. 190/2018)

66. Cine acreditează organismele de certificare?

Acreditarea organismelor de certificare prevăzute la art. 43 din Regulamentul general privind protecția datelor se realizează de Asociația de Acreditare din România – RENAR, în calitate de organism național de acreditare, în conformitate cu Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului din 9 iulie 2008, precum și în conformitate cu Ordonanța Guvernului nr. 23/2009 privind activitatea de acreditare a organismelor de evaluare a conformității, aprobată cu modificări prin Legea nr.

256/2011.
(art. 11 din Legea nr. 190/2018)

67. Ce măsuri poate lua autoritatea de supraveghere în sectorul privat în cazul în care constată încălcarea prevederilor Regulamentului (UE) 2016/679?

Sancţiunile contravenţionale principale pe care le aplică autoritatea de supraveghere în sectorul privat sunt **avertismentul** şi **amenda.**

În funcţie de circumstanţele fiecărui caz în parte, autoritatea de supraveghere aplică amenzi administrative de până la 10 000 000 – 20 000 000 EUR sau, în cazul unei întreprinderi, de până la 2 % - 4 % din cifra de afaceri mondială totală anuală corespunzătoare exerciţiului financiar anterior, luându-se în calcul cea mai mare valoare.

Pe lângă aplicarea sancţiunilor contravenţionale prevăzute de lege, autoritatea de supraveghere poate dispune şi alte măsuri corective şi poate formula recomandări.

Măsurile corective ce pot fi dispuse de către autoritatea de supraveghere, pot consta în:

- ⇒ obligarea operatorului sau a persoanei împuternicite de operator să respecte cererile persoanei vizate de exercitare a drepturilor, să asigure conformitatea operaţiunilor de prelucrare cu dispoziţiile legale aplicabile;
- ⇒ obligarea operatorului să informeze persoana vizată cu privire la o încălcare a protecţiei datelor cu caracter personal;
- ⇒ limitarea temporară sau definitivă, interdicţia asupra prelucrării, rectificarea sau ştergerea datelor cu caracter personal, restricţionarea prelucrării;
- ⇒ retragerea unei certificări sau obligarea organismului de certificare să retragă o certificare eliberată sau să nu elibereze o certificare în cazul în care cerinţele de certificare nu sunt sau nu mai sunt îndeplinite;
- ⇒ suspendarea fluxurilor de date către un destinatar dintr-o ţară terţă sau către o organizaţie internaţională

(art. 58 și art. 83 din RGPD)

68. Autorităţile şi organismele publice pot fi sancționate de autoritatea de supraveghere?

Sancțiunile contravenționale principale aplicate autorităților și organismelor publice sunt **avertismentul și amenda contravențională.**

În cazul constatării încălcării prevederilor Regulamentului general privind protecţia datelor şi ale Legii nr. 190/2018 de către autorităţile/organismele publice, **Autoritatea naţională de supraveghere poate aplica sancţiunea avertismentului**, la care anexează un **plan de remediere și stabilește un**

termen de aducere la îndeplinire a măsurilor dispuse.

Termenul de remediere se stabileşte în funcţie de riscurile asociate prelucrării, precum şi demersurile necesar a fi îndeplinite pentru asigurarea conformităţi prelucrării.

Planul de remediere este prevăzut în anexa la Legea nr. 190/2018. Acesta se anexează la procesul-verbal de constatare şi sancţionare a contravenţiei.

În situația în care autoritatea de supraveghere constată faptul că autorităţile/organismele publice nu au adus la îndeplinire în totalitate măsurile prevăzute în planul de remediere, în termenul stabilit de autoritate, aceasta poate aplica **sancţiunea contravenţională a amenzii de la 10.000 lei până la 200.000 lei.**

(art. 13 și 14 din Legea nr. 190/2018)

69. Ce decizii administrative cu caracter normativ a emis Autoritatea Națională de Supraveghere în anul 2018?

În vederea punerii în aplicare a Regulamentului (UE) 2016/679, Autoritatea Națională de Supraveghere a emis următoarele decizii administrative cu caracter normativ:

- ⇒ **Decizia nr. 99/2018** privind încetarea aplicabilităţii unor acte normative cu caracter administrativ emise în aplicarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date
- ⇒ **Decizia nr. 128/2018** privind aprobarea formularului tipizat al notificării de încălcare a securităţii datelor cu caracter personal în conformitate cu Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE
- ⇒ **Decizia nr. 133/2018** privind aprobarea Procedurii de primire și soluționare a plângerilor
- ⇒ **Decizia nr. 161/2018** privind aprobarea Procedurii de efectuare a investigațiilor
- ⇒ **Decizia nr. 174/2018** privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor cu caracter personal

De asemenea, a rămas în vigoare Decizia nr. 184/2014 privind aprobarea formularului tipizat al notificării de încălcare a securităţii datelor cu caracter personal pentru furnizorii de servicii publice de reţele sau servicii de comunicaţii electronice, în conformitate cu Regulamentul (UE) nr. 611/2013 al Comisiei din 24 iunie 2013 privind măsurile aplicabile notificării încălcărilor securităţii datelor cu caracter personal în temeiul Directivei 2002/58/CE a Parlamentului European

şi a Consiliului privind confidenţialitatea şi comunicaţiile electronice (publicată în Monitorul Oficial 964 din 30.12.2014).

70. Ce aspecte principale reglementează Decizia nr. 133/2018 privind aprobarea Procedurii de primire și soluționare a plângerilor?

Decizia nr. 133/2018 privind aprobarea Procedurii de primire și soluționare a plângerilor vizează, în principal, următoarele aspecte:

- ✓ **plângerile pot fi adresate de orice persoană vizată**, în special în cazul în care reşedinţa sa obişnuită, locul său de muncă sau presupusa încălcare se află sau, după caz, are loc pe teritoriul României;
- ✓ plângerile pot fi depuse la sediul Autorității de Supraveghere sau transmise prin poştă, inclusiv cea electronică, ori prin **utilizarea formularului electronic de plângere** disponibil pe pagina de internet a instituției https://www.dataprotection.ro/?page=Plangeri_RGPD&lang=ro;
- ✓ **plângerile pot fi depuse personal sau prin mandatar**, inclusiv prin intermediul unei organizaţii fără scop patrimonial, activă în domeniul protecţiei datelor lor cu caracter personal;
- ✓ **petiţionarii sunt informaţi în scris cu privire la admiterea plângerii**, inclusiv cu privire la efectuarea unei investigaţii mai amănunţite sau coordonarea cu alte autorităţi de supraveghere, precum și în legătură cu evoluţia sau cu rezultatul investigaţiei întreprinse;
- ✓ **persoana vizată nemulțumită de modalitatea de soluționare a plângerii sale se poate adresa secţiei de contencios administrativ a tribunalului competent**, după parcurgerea procedurii prealabile prevăzute de Legea contenciosului administrativ nr. 554/2004, cu modificările şi completările ulterioare.

71. Cine poate adresa o plângere la autoritatea de supraveghere?

Plângerile pot fi adresate de orice persoană vizată, care consideră că prelucrarea datelor sale cu caracter personal încalcă prevederile legale în vigoare, în special în cazul în care reşedinţa sa obişnuită, locul său de muncă sau presupusa încălcare se află sau, după caz, are loc pe teritoriul României.

72. Care sunt condițiile de adresare a unei plângeri?

Plângerile trebuie formulate în scris, în limba română sau engleză.

Plângerile pot fi depuse la registratura generală de la sediul autorității de supraveghere sau pot fi transmise prin poştă, inclusiv cea electronică, ori prin utilizarea formularului electronic, disponibil pe pagina de internet a autorității de supraveghere, la secțiunea Plângeri.

Anterior depunerii unei plângeri la autoritatea de supraveghere, persoanele vizate îți pot exercita drepturile prevăzute la Capitolul III din Regulamentul (UE) 2016/679. Potrivit art. 12 alin. (3) din RGPD, operatorul

furnizează persoanei vizate informaţii privind acţiunile întreprinse în urma unei cereri în temeiul articolelor 15-22, fără întârzieri nejustificate şi în orice caz *în cel mult o lună de la primirea cererii.*

Pentru mai multe informații, vă recomandăm să consultați *Decizia nr. 133/2018 a președintelui Autorității Naționale de Supraveghere privind aprobarea Procedurii de primire și soluționare a plângerilor*, disponibilă pe site-ul autorității www.dataprotection.ro .

73. Plângerile pot fi depuse și de alte persoane decât persoana vizată?

Plângerile pot fi depuse personal sau prin reprezentant, cu anexarea împuternicirii emise în condiţiile legii de un avocat sau a procurii notariale, după caz.

Plângerile pot fi depuse şi de către mandatarul persoanei vizate care este soţ sau rudă până la gradul al doilea inclusiv, anexând o declaraţie pe propria răspundere semnată de petiţionar, iar în cazul altor persoane, o procură notarială.

Plângerile pot fi depuse și prin intermediul unui organism, al unei organizaţii, al unei asociaţii sau fundaţii fără scop patrimonial. Acestea trebuie să dovedească faptul că au fost constituite legal, cu un statut ce prevede obiective de interes public, şi că sunt active în domeniul protecţiei drepturilor şi libertăţilor persoanelor vizate în ceea ce priveşte protecţia datelor lor cu caracter personal. În acest caz, la plângere se anexează inclusiv împuternicirea avocaţială sau procura notarială de reprezentare, după caz, din care să rezulte limitele mandatului acordat de persoana vizată, precum şi statutul organismului/organizaţiei/asociaţiei/fundaţiei, precum şi dovezi privind activitatea acestora în domeniul protecţiei drepturilor şi libertăţilor persoanelor vizate în ceea ce priveşte protecţia datelor lor cu caracter personal.

Pentru mai multe informații, vă recomandăm să consultați *Decizia nr. 133/2018 a președintelui Autorității Naționale de Supraveghere privind aprobarea Procedurii de primire și soluționare a plângerilor*, disponibilă pe site-ul autorității www.dataprotection.ro .

74. Autoritatea de supraveghere poate percepe taxă pentru primirea și analizarea plângerilor?

Primirea plângerilor la autoritatea de supraveghere şi analizarea acestora este, de regulă, gratuită.

În cazul în care plângerile sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, *autoritatea poate percepe o taxă rezonabilă*, bazată pe costurile administrative, sau poate refuza să le trateze.

Pentru mai multe informații, vă recomandăm să consultați *Decizia nr. 133/2018 a președintelui Autorității Naționale de Supraveghere privind*

aprobarea Procedurii de primire și soluționare a plângerilor, disponibilă pe site-ul autorității www.dataprotection.ro .

75. Petiționarii pot solicita păstrarea confidențialității anumitor date cu caracter personal?

Petiţionarii pot solicita păstrarea confidenţialităţii anumitor date cu caracter personal, menţionate în mod expres, furnizate prin plângere, *cu excepţia situaţiilor* în care, pentru soluţionarea corespunzătoare a obiectului plângerilor depuse, datele de identificare ale petiţionarului trebuie să fie dezvăluite către entitatea reclamată.

Pentru mai multe informații, vă recomandăm să consultați *Decizia nr. 133/2018 a președintelui Autorității Naționale de Supraveghere privind aprobarea Procedurii de primire și soluționare a plângerilor*, disponibilă pe site-ul autorității www.dataprotection.ro .

76. Când este admisibilă o plângere?

Pentru primirea şi înregistrarea valabilă a plângerilor *este obligatorie* furnizarea următoarelor date ale *petiţionarului*: nume, prenume, adresă poştală de domiciliu sau de reşedinţă.

În cazul în care plângerea este depusă electronic este obligatorie furnizarea adresei de poştă electronică a petiţionarului.

În cazul plângerilor înaintate prin reprezentant, în afara datelor petiţionarului este obligatorie şi furnizarea următoarelor date ale reprezentantului: *nume şi prenume/denumire, adresă poştală de corespondenţă/sediu, adresă de poştă electronică, număr de telefon, număr de înregistrare în registrul asociaţiilor şi fundaţiilor*, dacă este cazul.

Pentru primirea şi înregistrarea valabilă a plângerilor *este obligatorie* furnizarea datelor de identificare ale *operatorului reclamat* sau a persoanei împuternicite reclamate, precum nume şi prenume/denumire, adresă/sediu, sau cel puţin a informaţiilor disponibile deţinute de petiţionar, în vederea identificării acestora.

Plângerile trimise *se semnează olograf sau electronic*, iar în cazul petiţiilor trimise electronic care nu pot fi semnate, Autoritatea Națională de Supraveghere poate solicita confirmarea corectitudinii datelor transmise electronic.

Pentru mai multe informații, vă recomandăm să consultați *Decizia nr. 133/2018 a președintelui Autorității Naționale de Supraveghere privind aprobarea Procedurii de primire și soluționare a plângerilor*, disponibilă pe site-ul autorității www.dataprotection.ro.

77. Care este termenul de răspuns al autorității de supraveghere la plângerile depuse?

Autoritatea de supraveghere informează persoana vizată cu privire la admisibilitatea plângerii, în termen de cel mult 45 de zile de la înregistrare.

În cazul în care se constată că informațiile din plângere sau documentele transmise sunt incomplete sau insuficiente, Autoritatea Națională de Supraveghere solicită persoanei vizate să completeze plângerea pentru a putea fi considerată admisibilă în vederea efectuării unei investigații. Un nou termen de cel mult 45 de zile curge de la data completării plângerii.

Autoritatea Națională de Supraveghere informează persoana vizată în legătură cu evoluția sau cu rezultatul investigației întreprinse în termen de 3 luni de la data la care s-a comunicat acesteia că plângerea este admisibilă.

Pentru mai multe informații, vă recomandăm să consultați *Decizia nr. 133/2018 a președintelui Autorității Naționale de Supraveghere privind aprobarea Procedurii de primire și soluționare a plângerilor*, disponibilă pe site-ul autorității www.dataprotection.ro.

78. Persoanele vizate au dreptul de a se adresa instanței competente pentru apărarea drepturilor care le-au fost încălcate?

Fără a se aduce atingere posibilității de a se adresa cu plângere Autorității Naționale de Supraveghere, persoanele vizate au dreptul de a se adresa instanței competente pentru apărarea drepturilor garantate de legislația aplicabilă, care le-au fost încălcate.

În cazul în care a fost introdusă *o cerere în justiție cu același obiect și având aceleași părți*, autoritatea de supraveghere *poate dispune suspendarea sau/și clasarea plângerii*, după caz.

Persoana vizată va trebui să informeze Autoritatea, prin intermediul formularului de plângere, cu privire la introducerea unei asemenea cereri în justiție.

79. În ce condiții se aplică Regulamentul (UE) 2016/679 plângerilor și sesizărilor depuse și înregistrate la autoritatea de supraveghere?

Dispozițiile Regulamentului general privind protecția datelor se aplică:

- ✓ *plângerilor și sesizărilor depuse și înregistrate la Autoritatea Națională de Supraveghere după 25 mai 2018;*
- ✓ *plângerilor și sesizărilor depuse înainte de 25 mai 2018 și aflate în curs de soluționare;*
- ✓ *investigațiilor efectuate pentru soluționarea plângerilor și sesizărilor și investigațiilor din oficiu, inclusiv celor începute anterior datei de 25 mai 2018 și nefinalizate la această dată.*

(art. VI din Legea nr. 129/2018)

80. Când poate fi clasată o plângere?

Plângerea în care nu se precizează datele de identificare ale petiţionarului (nume, prenume, adresă poştală de domiciliu sau de reşedinţă) este considerată anonimă şi se clasează cu această menţiune, fără a se formula un răspuns petiţionarului.

Pentru mai multe informații, vă recomandăm să consultați Decizia nr. 133/2018 a președintelui Autorității Naționale de Supraveghere privind aprobarea Procedurii de primire și soluționare a plângerilor, disponibilă pe site-ul autorității www.dataprotection.ro.

81. Ce aspecte reglementează Decizia nr. 161/2018 privind aprobarea Procedurii de efectuare a investigațiilor?

Decizia nr. 161/2018 privind aprobarea Procedurii de efectuare a investigațiilor stabilește condițiile de desfășurare a investigațiilor pe teren, la sediul autorității de supraveghere și a celor derulate în scris, precum și efectuarea acestora la autoritățile/organismele publice.

Investigația se poate finaliza cu întocmirea unui proces-verbal de constatare/sancționare sau a unei decizii a Președintelui Autorității Naționale de Supraveghere, prin care se pot dispune măsuri corective și/sau sancțiuni contravenționale (avertisment, amendă).

În cazul autorităților/organismelor publice, anterior acordării unei sancțiuni pecuniare se aplică avertisment și se întocmește un plan de remediere potrivit modelului prevăzut de Legea nr. 190/2018 și care trebuie îndeplinit în termenul acordat de autoritatea de supraveghere.

Măsurile dispuse pot fi contestate în termen de 15 zile la secția de contencios administrativ a tribunalului competent.

Pentru mai multe informații, vă recomandăm să consultați *Decizia nr. 161/2018 a președintelui Autorității Naționale de Supraveghere privind aprobarea Procedurii de efectuare a investigațiilor*, disponibilă pe site-ul autorității www.dataprotection.ro.

82. Când efectuează autoritatea de supraveghere investigații?

Autoritatea de supraveghere efectuează investigaţii din oficiu sau la plângere.

Investigaţiile din oficiu se efectuează pentru verificarea unor date şi informaţii cu privire la prelucrarea datelor cu caracter personal, obţinute de către Autoritatea Naţională de Supraveghere din alte surse decât cele care fac obiectul unor plângeri.

Investigaţiile se pot efectua şi pentru soluţionarea plângerilor primite de

Autoritatea Națională de Supraveghere.

Pentru mai multe informații, vă recomandăm să consultați *Decizia nr. 161/2018 a președintelui Autorității Naționale de Supraveghere privind aprobarea Procedurii de efectuare a investigațiilor*, disponibilă pe site-ul autorității www.dataprotection.ro.

83. Care este modalitatea de efectuare a investigațiilor?

Investigaţiile pot fi efectuate pe teren, la sediul autorităţii ori în scris.

Investigaţiile pe teren constau în verificări efectuate la sediul/domiciliul/punctul de lucru sau alte locaţii unde îşi desfăşoară activitatea entitatea controlată sau locaţii care au legătură cu prelucrarea în cauză, după caz.

Investigaţia nu poate începe înainte de ora 8,00 şi nu poate continua după ora 18,00 și trebuie efectuată în prezenţa persoanei la care se efectuează investigaţia sau a reprezentantului său. Investigaţia poate continua şi după ora 18,00 numai cu acordul persoanei la care se efectuează aceasta sau a reprezentantului său.

În cazul investigaţiilor efectuate la sediul Autoritatea Națională de Supraveghere, personalul de control desemnat transmite o adresă de convocare a reprezentanţilor entităţii controlate, cu precizarea datei şi orei de începere a investigaţiei.

În cazul investigaţiilor în scris, se transmite o adresă către entitatea controlată, prin care se solicită informaţii, date şi documente necesare soluţionării cazului supus investigaţiei.

Pentru mai multe informații, vă recomandăm să consultați Decizia nr. 161/2018 a președintelui Autorității Naționale de Supraveghere privind aprobarea Procedurii de efectuare a investigațiilor, precum și capitolul IV din Legea 102/2005, republicată, disponibile pe site-ul autorității www.dataprotection.ro.

84. Care sunt obligațiile entității controlate în cazul investigațiilor efectuate pe teren?

În cadrul investigaţiei efectuată pe teren, entitatea controlată are, în principal, următoarele obligaţii:

- să permită personalului de control, fără întârziere, începerea şi derularea investigaţiei şi să asigure suportul necesar personalului de control;
- să asigure accesul personalului de control în incintele în care îşi desfăşoară activitatea, la orice echipament, mijloc sau suport de prelucrare/stocare a datelor, în vederea efectuării verificărilor necesare desfăşurării investigaţiei, inclusiv la cele care pot fi accesate la distanţă;
- să pună la dispoziţia personalului de control orice informaţii şi documente

indiferent de suportul de stocare, necesare desfăşurării investigaţiei, inclusiv copii de pe acestea;

- să pună la dispoziția Autorității Naționale de Supraveghere documentele solicitate, certificate pentru conformitate cu originalul;
- să furnizeze într-o formă completă documentele, informaţiile, înregistrările şi evidenţele solicitate, precum şi orice lămuriri necesare, fără a putea opune caracterul confidenţial al acestora, în condiţiile legii;
- să permită personalului de control utilizarea echipamentelor de înregistrare şi stocare audiovideo/foto ori de câte ori echipa de control consideră că este necesar în cadrul derulării activităţii de control.
- Împotriva procesului-verbal de constatare/ sancţionare şi/sau a deciziei de aplicare a măsurilor corective, după caz, operatorul sau persoana împuternicită de operator poate introduce contestaţie la secţia de contencios administrativ a tribunalului competent, în termen de 15 zile de la înmânare, respectiv de la comunicare. Hotărârea prin care s-a soluţionat contestaţia poate fi atacată numai cu apel. Apelul se judecă de curtea de apel competentă. În toate cazurile, instanţele competente sunt cele din România.

Pentru mai multe informații, vă recomandăm să consultați Decizia nr. 161/2018 a președintelui Autorității Naționale de Supraveghere privind aprobarea Procedurii de efectuare a investigațiilor, precum și capitolul IV din Legea 102/2005, disponibile pe site-ul autorității www.dataprotection.ro.

85. Cum sunt considerate referirile la Legea nr. 677/2001 din legislația națională?

Toate trimiterile la Legea nr. 677/2001, cu modificările şi completările ulterioare, din actele normative naționale se interpretează ca trimiteri la Regulamentul general privind protecţia datelor şi la legislaţia de punere în aplicare a acestuia.

Notes

AUTORITATEA NAȚIONALĂ DE SUPRAVEGHERE A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

romania2019.eu
Președinția României la Consiliul Uniunii Europene

ANS
PDCP