



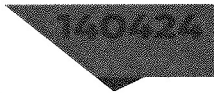
UNIUNEA EUROPEANĂ



Instrumente Structurale
2014-2020

CONFORMITATE CU GDPR. DE UNDE INCEPEM?

Proiect „ARC -Anteprenoriat, Responsabilitate, Creativitate” POCU/829/6/13/140424



Proiect cofinanțat din Fondul Social European prin Programul Operațional Capital Uman 2014 - 2020
Axa prioritara 6 - Educație și competențe;
Obiectivul specific 6.13 Creșterea numărului absolvenților de învățământ terțiar universitar și non universitar care își găsesc un loc de muncă urmare a
accesului la activități de inovare în un potențial loc de muncă / cercetare / inovare, cu accent pe sectoarele economice cu potențial competitiv identificate
conform SNC și domeniile de specializare inteligente conform SNCII
Titlul proiectului " ARC - Anteprenoriat, Responsabilitate, Creativitate"
Contract POCU/ 829 / 6 / 13 / 140424
Beneficiar: Asociația Getica



ASOCIAȚIA
GETICA



Formprof
Servicii

Begli
Event

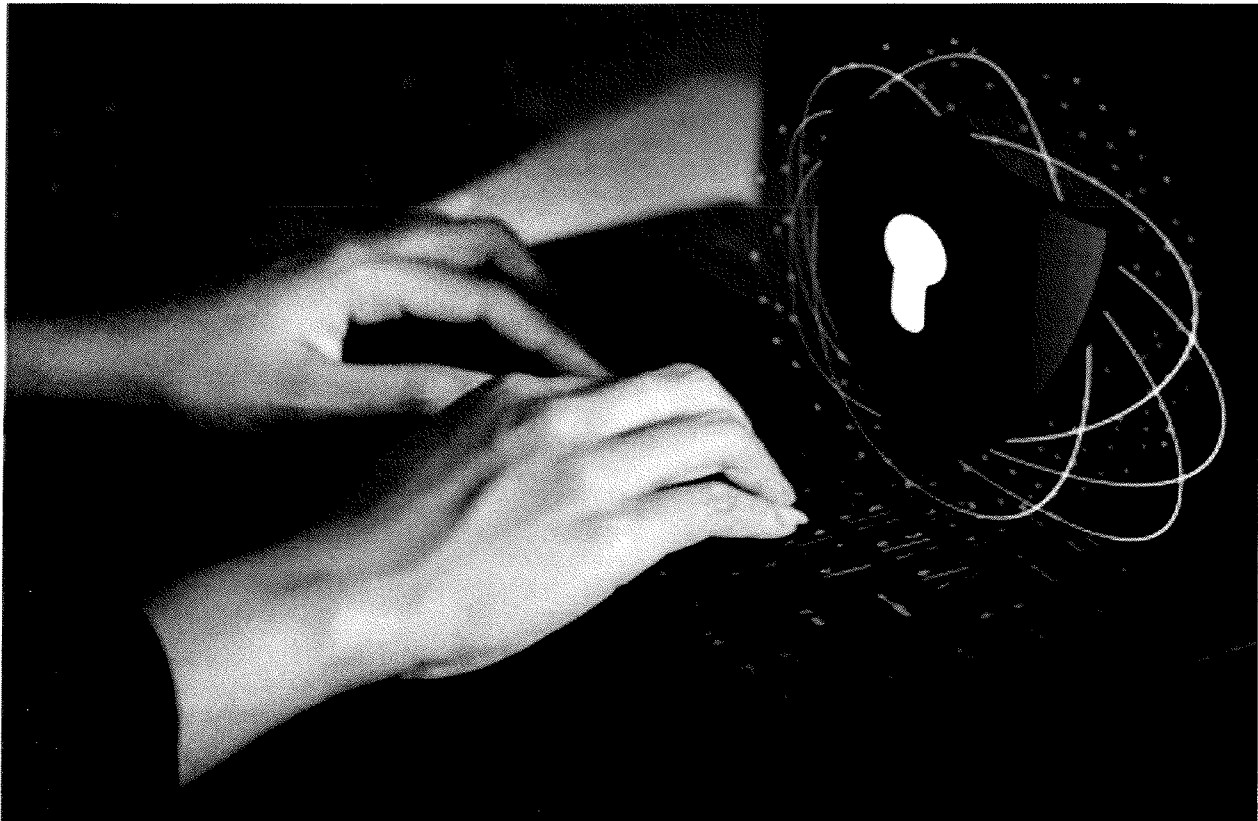


UNIUNEA EUROPEANĂ



Instrumente Structurale
2014-2020

REGULAMENTUL GENERAL PRIVIND PROTECȚIA DATELOR



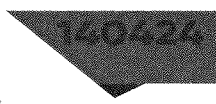
Despre ce discutăm?

Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor - GDPR) s-a aplicat începând cu data de 25 mai 2018. Regulamentul este un act legislativ cu caracter obligatoriu. Trebuie aplicat în integralitatea sa, în toate statele membre.

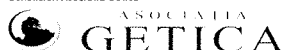
În România, avem următoarele proiecte de lege:

- Proiectul de lege pentru modificarea și completarea Legii nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum și pentru abrogarea Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date. - adoptat de Camera Deputaților – prioritate legislativă

1



Proiect cofinanțat din Fondul Social European prin Programul Operațional Capital Uman 2014 - 2020
Axa prioritară 6 - Educație și competențe
Obiectivul specific 6.13 Creșterea numărului absolvenților de învățământ terțiar universitar și non universitar care își găsesc un loc de muncă urmarea a
accesului la activități de învățare la un potențial loc de muncă / cercetare / inovare, cu accent pe sectoarele economice cu potențial competitiv identificate
conform SNC și domeniile de specializare inteligentă conform SNCII
Titlul proiectului " ARD - Antreprenoriat, Responsabilitate, Creativitate"
Contract: POCU/839/6/15/140424
Beneficiar: Asociația Getica





UNIUNEA EUROPEANĂ



Instrumente Structurale
2014-2020

a Guvernului - procedură de urgență - înscris pe ordinea de zi a Senatului din data de 22.05.2018 pentru vot final, cameră decizională

- Propunere legislativă privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/EC (Regulamentul general privind protecția datelor) - în lucru, la comisiile permanente ale Senatului Indiferent de soluția propunerilor de lege, GDPR se va aplica.

Despre ale cui date personale vorbim?

Carta Drepturilor Fundamentale a Uniunii Europene se referă doar la drepturile persoanelor fizice. La fel și art. 8 din Carta, care prevede: Protecția datelor cu caracter personal (1) Orice persoană are dreptul la protecția datelor cu caracter personal care o privesc. (2) Asemenea date trebuie tratate în mod corect, în scopurile precizate și pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege. Orice persoană are dreptul de acces la datele colectate care o privesc, precum și dreptul de a obține rectificarea acestora. (3) Respectarea acestor norme se supune controlului unei autorități independente. Deși textul nu precizează, este vorba despre persoane fizice. În schimb, Regulamentul (UE) 2016/679 se referă explicit la protecția datelor cu caracter personal ale persoanelor fizice, excluzând explicit de la protecția sa datele cu caracter personal ale persoanelor juridice, precum și o seamă de situații de prelucrare a datelor cu caracter personal ale persoanelor fizice, numeroase și importante.

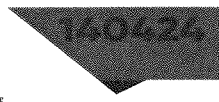
Dreptul la protecția datelor personale este un drept?

Deși textul se referă la dreptul la protecția datelor cu caracter personal, el figurează în Cartă sub titlul LIBERTĂȚII. Regulamentul se referă dreptul la protecția datelor cu caracter personal ca fiind un drept fundamental, însă, precizează Regulamentul, el trebuie luat în considerare în raport cu funcția pe care o îndeplinește în societate și echilibrat cu alte drepturi fundamentale, în conformitate cu principiul proporționalității (pct. 4 din expunerea de motive a Regulamentului).

Potrivit acestui principiu, pot fi impuse restrângeri numai în cazul în care acestea sunt necesare și numai dacă răspund efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților (art. 52 alin. 1 din Cartă). În orice caz, dreptul la protecția datelor cu caracter personal nu este un drept absolut, nici în concepția Regulamentului, nici în sensul utilizat în dreptul românesc, de drept căruia îi corespunde obligația generală de a nu stânjeni titularul dreptului.

Dreptul la protecția datelor cu caracter personal este ceva foarte special?

Dreptul la protecția datelor cu caracter personal avute în vedere de Regulament este special, întrucât necesită o conduită activă din partea altcuiva. Dar nu este singurul în această situație ingrată. Realizarea conținutului acestui drept necesită un efort din partea altcuiva. Eforturile costă.





UNIUNEA EUROPEANĂ



Cine suportă costurile protecției datelor personale?

Regulamentul pune aceste costuri în sarcina celui alt, nu în sarcina titularului dreptului (art. 12 alin. 4 din Regulament).

Pentru cine este important Regulamentul?

Pentru toate organizațiile, indiferent de forma de proprietate, care prelucrează date cu caracter personal.

Ce înseamnă prelucrarea datelor cu caracter personal?

Din păcate, „prelucrarea” are o definiție chiar în cuprinsul Regulamentului (art. 2 pct. 2 RGPD). În înțelesul Regulamentului, prelucrare înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea. Adică orice atingere, cât de mică.

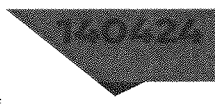
Regulamentul se aplică oricăror prelucrări de date cu caracter personal?

Nu chiar, dar aproape tuturor... Art. 2 nu lasă mult loc pentru a evita aplicarea Regulamentului. Iată: “(1) Prezentul regulament se aplică prelucrării datelor cu caracter personal, efectuată total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor. (2) Prezentul regulament nu se aplică prelucrării datelor cu caracter personal:

- (a) în cadrul unei activități care nu intră sub incidența dreptului Uniunii;
- (b) de către statele membre atunci când desfășoară activități care intră sub incidența capitolului 2 al titlului V din Tratatul UE; (politică de securitate și apărare comună);
- (c) de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice;
- (d) de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmării penale a infracțiunilor, sau al executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora.”

De ce este important Regulamentul?

Din pricina (i) felului în care reglementează tragerea la răspundere și din pricina (ii) sancțiunilor foarte aspre.





UNIUNEA EUROPEANĂ



Cine poate să tragă la răspundere operatorii de date personale?

Oricine, orice persoană fizică. Orice persoană vizată are dreptul de a depune o plângere la autoritatea națională de supraveghere, în special în statul membru în care își are reședința obișnuită, în care se află locul său de muncă sau în care a avut loc presupusa încălcare, în cazul în care consideră că prelucrarea datelor cu caracter personal care o vizează încalcă regulamentul (art. 77 RGPD).

Există sancțiuni penale?

Din fericire, Regulamentul nu instituie sancțiuni penale, și nici nu ar putea, întrucât reglementările europene nu instituie sancțiuni penale. Însă nerespectarea dispozițiilor Regulamentului poate atrage răspunderea penală, de exemplu în cadrul infracțiunii de abuz în serviciu.

Dar sancțiuni civile?

Regulamentul nu prevede sancțiuni civile, însă reglementează într-un mod foarte împovăraător modul în care intervine răspunderea civilă în cazul încălcării prevederilor lui. Orice persoană care a suferit un prejudiciu material sau moral ca urmare a unei încălcări a RGPD are dreptul să obțină despăgubiri de la operator (art. 82 alin. 1 RGPD) și, corelativ, orice operator implicat în operațiunile de prelucrare este răspunzător pentru prejudiciul cauzat de operațiunile sale de prelucrare care încalcă RGPD (art. 82 alin. 2 RGPD).

Dar sancțiuni administrative (amenzi)?

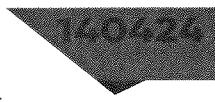
Da, foarte periculoase. Acesta este de altfel motivul pentru care Regulamentul a devenit celebru și constituie o preocupare importantă în toate țările Uniunii Europene. În concepția RGPD, sancțiunile civile.

Când este legală prelucrare?

Prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții (art. 6 alin. (1) GDPR):

- a) persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;
- b) 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;
- c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;
- d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;

4



Proiect cofinanțat din Fondul Social European prin Programul Operațional Capital Uman 2014 – 2020
Axa prioritară 6 – Educație și competențe
Obiectivul specific 6.13 Creșterea numărului absolvenților de învățământ terțiar universitar și non universitar care își găsesc un loc de muncă urmare a accesului la activități de inovare la un potențial loc de muncă / cercetare / inovare, cu accent pe sectoarele economice cu potențial competitiv identificate conform SNC și domeniile de specializare inteligente conform SNCII
Titlul proiectului - ARC - Antreprenoriat, Responsabilitate, Creativitate
Contract: POCU/6.13/140424
Beneficiar: Asociația Getica



e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul;

f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de 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.

OPERATORII CARE PRELUCREAZĂ DATE CU CARACTER PERSONAL



Cine sunt operatorii? Cui i se aplică Regulamentul?

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 (art. 4 pct. (7) GDPR). Cu alte cuvinte, operator este cel pentru care se realizează prelucrarea datelor, chiar dacă operatorul nu realizează el însuși nicio prelucrare.



UNIUNEA EUROPEANĂ



Cine este operator de date personale?

Orice prelucrare a datelor cu caracter personal în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator din Uniune ar trebui efectuată în conformitate cu Regulamentul, indiferent dacă procesul de prelucrare în sine are loc sau nu în cadrul Uniunii. Prelucrarea datelor cu caracter personal ale persoanelor vizate care se află pe teritoriul Uniunii de către un operator sau o persoană împuternicită de acesta care nu își are sediul în Uniune face obiectul regulament în cazul în care este legată de monitorizarea comportamentului unor astfel de persoane vizate, în măsura în care acest comportament se manifestă pe teritoriul Uniunii (pct. 24 EM), ceea ce este cazul în speță.

Cine este operator asociat de date personale?

Dacă operatorul colaborează cu privire la atragerea de clienți cu alte entități, adică acestea și operatorul stabilesc în comun scopurile și mijloacele de prelucrare, atunci sunt operatori asociați (art. 26 alin. (1) RGPD). Trebuie stabilite într-un mod transparent responsabilitățile fiecăruia în ceea ce privește îndeplinirea obligațiilor care le revin în temeiul RGPD, 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. Esența acestui acord este făcută cunoscută persoanei vizate (art. 26 alin. (2) RGPD). În orice caz, indiferent de clauzele acordului, persoana vizată își poate exercita drepturile chiar și direct, în temeiul RGPD, cu privire la și în raport cu fiecare dintre operatori (art. 26 alin. (3) RGPD).

Cine trebuie să țină evidența prelucrărilor de date cu caracter personal?

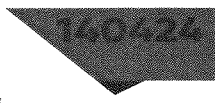
Fiecare operator trebuie să păstreze evidența activităților de prelucrare desfășurate sub responsabilitatea lui și în numele lui, evidențe care trebuie să cuprindă informațiile prevăzute de art. 30 alin. (1) lit. (a)-(g) și, respectiv, alin. (2) lit. (a)-(d) RGPD. Această evidență este necesară întrucât autoritatea de supraveghere poate să ceară oricând acces la ea (art. 30 alin. 4 RGPD).

Totuși, chiar și organizațiile mici trebuie să țină evidența prelucrărilor de date cu caracter personal?

Obligațiile privind ținerea evidenței prelucrărilor de date cu caracter personal nu se aplică organizațiilor cu mai puțin de 250 de angajați, cf. art. 30 alin. (5) RGPD.

Atenție, această prevedere este reglementată cu titlu de regulă. Excepțiile de la regulă sunt reglementate foarte larg, atât de largă încât în realitate nici organizațiile mici nu se pot sustrage de la îndeplinirea acestei obligații. Iată excepțiile, adică situațiile în care evidența este obligatorie și pentru organizațiile mici:

6



Proiect cofinanțat din Fondul Social European prin Programul Operațional Capital Uman 2014 – 2020
Axa prioritară 6 – Educație și competențe
Obiectivul specific 6.13 Creșterea numărului absolvenților de învățământ terțiar universitar și non universitar care își găsesc un loc de muncă urmare a accesului la activități de inovare la un potențial loc de muncă / cercetare / inovare, cu accent pe sectoarele economice cu potențial competitiv identificate conform SNC și domeniile de specializare inteligente conform SNCII
Titlul proiectului "ARC – Antreprenoriat, Responsabilitate, Creativitate"
Contractul POCSU/829/6/17/10424
Beneficiar: Asociația Getica





UNIUNEA EUROPEANĂ



- prelucrarea este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate
- prelucrarea nu este ocazională
- prelucrarea include categorii speciale de date, astfel cum se prevede la articolul 9 alineatul (1), sau date cu caracter personal referitoare la condamnări penale și infracțiuni, astfel cum se menționează la articolul 10. Excepția marcată cu roșu evidențiază ca dacă prelucrarea datelor personale este non-ocazională, atunci obligația de ținere a evidenței există.

Ce date personale putem să colectăm?

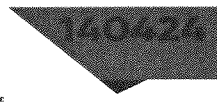
Orice date personale, însă doar în măsura în care sunt necesare pentru realizarea activității. Este foarte importantă lista (enumerarea) datelor cu caracter personal care sunt colectate. „Date cu caracter personal” înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale. (art. 4 pct. 1 RGPD)

Ce înseamnă securitatea prelucrării?

GDPR cere operatorilor să implementeze măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător (art. 32 RGPD), referitoare la:

- a) pseudonimizarea și criptarea datelor cu caracter personal;
- b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;
- c) capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- d) un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării. Această enumerare nu este limitativă.

IMPORTANT! Trebuie realizată și implementată o procedură tehnică de securizare a circuitului colectării, păstrării, prelucrării și ștergerii datelor cu caracter personal, inclusiv criptare, reglementare și implementare drepturi de acces, circuitul datelor, organizarea accesului, precum și audit de organizare și tehnic, pentru evaluarea riscurilor de securitate.





UNIUNEA EUROPEANĂ



Cât timp putem să stocăm datele personale?

Stabilirea perioadei pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă. În speță, sugerez stabilirea unui interval de timp de la ultima utilizare a unui produs, de exemplu ultima cumpărare realizată online sau ultima accesare a unui cont de acces privilegiat. Această informație trebuie să fie comunicată persoanelor vizate. Operatorul trebuie să stabilească prin decizie internă termenele de stocare și procedura de colectare, revizuire și ștergere a datelor personale. Colectarea, revizuirea și ștergerea se pot realiza automat, însă procedura stabilită prin decizie internă trebuie să prevadă și modalitățile și termenele de verificare.

Este nevoie de proceduri speciale pentru DATA PROTECTION?

Întreaga activitate a operatorului ar trebui să fie atent procedurată, cu integrare atentă în procedurile de lucru deja existente a regulilor în materia protecției datelor cu caracter personal.

Pe scurt, ce-i de făcut?

Pe fond, operatorii au de făcut 3 lucruri importante:

1. să-și adapteze procedurile de lucru, pentru ca accesul la date să fie cât mai limitat și cât mai securizat
2. să securizeze informatic datele personale
3. să încheie acorduri cu operatorii asociați

Procedural, operatorii trebuie:

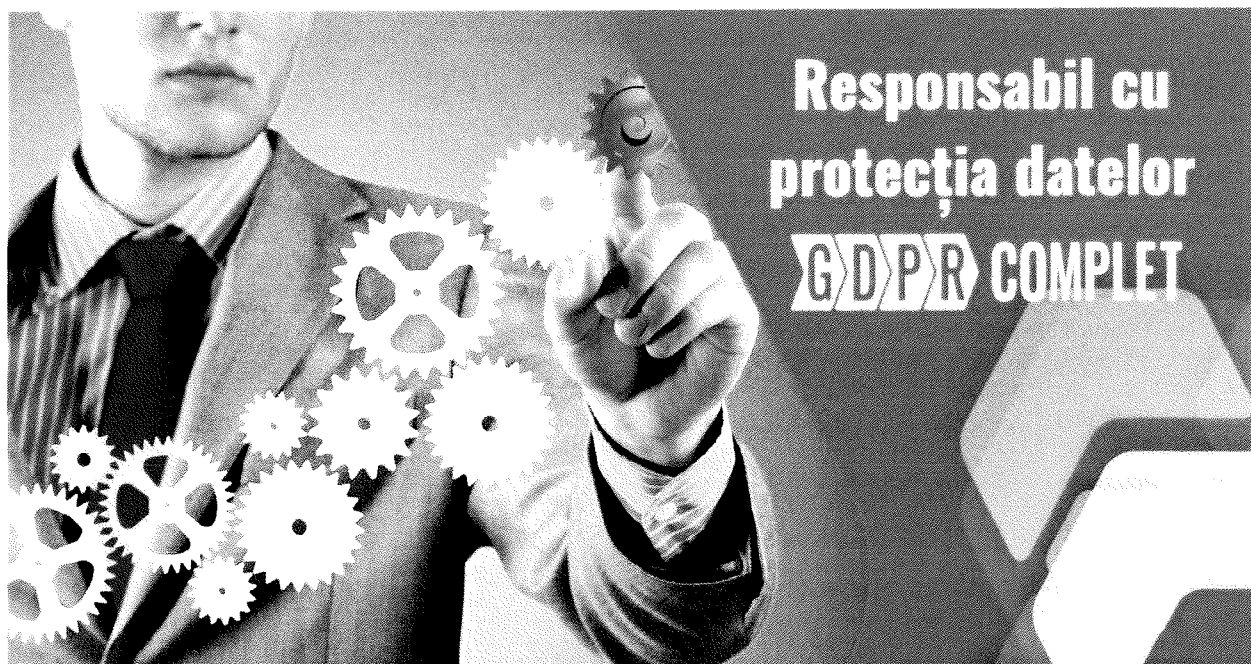
- a. să își aleagă un responsabil pentru protecția datelor personale
- b. să țină evidența prelucrărilor de date personale



UNIUNEA EUROPEANĂ



RESPONSABILUL CU PROTECȚIA DATELOR PERSONALE



Cine poate să apeleze la un “responsabil cu protecția datelor”? Cine trebuie să apeleze la un “responsabil cu protecția datelor”?

Oricine poate să apeleze la un responsabil cu protecția datelor personale. Operatorii trebuie să desemneze un responsabil cu protecția datelor atunci când printre altele, activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrare care, prin natura, domeniul de aplicare și/sau scopurile lor, necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă (art. 37 alin. 1 lit. b) RGPD). Pe larg, cf. art. 37 alin. (1), operatorul desemnează un responsabil cu protecția datelor ori de câte ori:

- a) prelucrarea este efectuată de o autoritate sau un organism public, cu excepția instanțelor care acționează în exercițiul funcției lor jurisdicționale;
- b) activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrare care, prin natura, domeniul de aplicare și/sau scopurile lor, necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă; sau
- c) 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.



UNIUNEA EUROPEANĂ



Cine este responsabilul cu protecția datelor personale?

Responsabilul cu protecția datelor trebuie să fie desemnat (art. 37 alin. 5 RGPD) pe baza calităților profesionale și, în special, a cunoștințelor de specialitate în dreptul și practicile din domeniul protecției datelor, precum și pe baza capacității de a îndeplini următoarele sarcini:

i) informarea și consilierea operatorului, sau a persoanei împuternicite de operator, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul RGPD și al altor dispoziții de drept al Uniunii sau drept intern referitoare la protecția datelor;

ii) monitorizarea respectării prezentului regulament, a altor dispoziții de drept al Uniunii sau de drept intern referitoare la protecția datelor și a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;

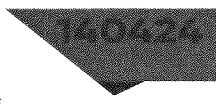
iii) furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării protecției datelor;

iv) cooperarea cu autoritatea națională de supraveghere;

v) asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune (art. 39 alin. 1 RGPD). Responsabilul cu protecția datelor poate fi un membru al personalului operatorului sau persoanei împuternicite de operator sau poate să își îndeplinească sarcinile în baza unui contract de servicii (art. 37 alin. 6). Observație semantică foarte importantă: *Responsabilul cu protecția datelor personale nu este persoana care preia responsabilitatea protecției datelor, aceasta rămâne în sarcina operatorului. Responsabilul este denumit așa în virtutea atribuțiilor sale.*

Dacă datele cu caracter personal sunt securizate atât la nivel informatic, de departamentul IT, cât și pe suport scris, ce calificare ar trebui să aibă persoana responsabilă cu protecția datelor cu caracter personal?

Regulamentul nu cere o calificare specială pentru DPO, iar coduri oficiale de bune practici încă nu există. Responsabilul cu protecția datelor personale ar trebui să fie o persoană cu studii juridice, care să fie bine conectat la noutățile în domeniu, căci vor fi multe în următorii ani. Deopotrivă, DPO ar trebui să fie o persoană foarte organizată, care cunoaște foarte bine procedurile companiei, și care are și abilități tehnice, care înțelege ușor procesele. În plus, și foarte important, DPO trebuie să aibă foarte bune abilități de comunicare, atât cu persoanele vizate cât și, mai ales, cu Autoritatea (ANSPDCP).





UNIUNEA EUROPEANĂ

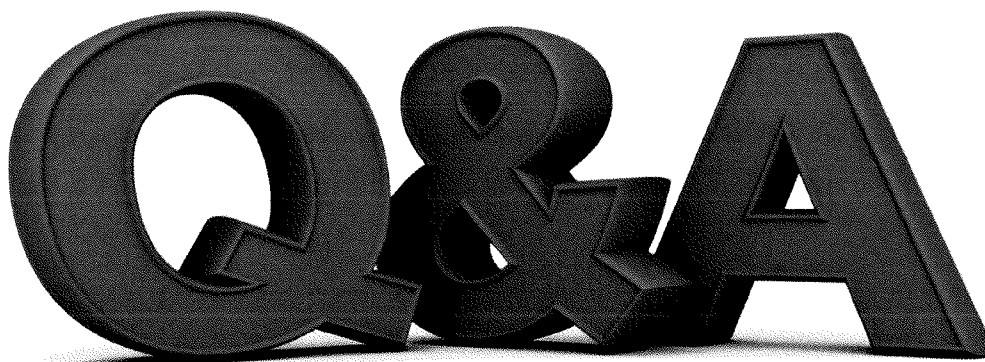


Instrumente Structurale
2014-2020

Este permisă desemnarea unui unic responsabil pentru protecția datelor personale pentru mai multe întreprinderi dintr-un grup?

Da, cu condiția ca el să fie ușor accesibil din fiecare întreprindere.

ÎNTREBĂRI ȘI RĂSPUNSURI



Ce înseamnă, cu precizie, "date personale"? „Date cu caracter personal” înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.

Practic, orice informație care poate duce la identificarea unei anumite persoane fizice reprezintă dată cu caracter personal. Enumerarea datelor cu caracter personal nu poate să fie limitativă. Datele personale sunt date dinamice datorită tehnologiei în continuă dezvoltare. Astfel, în viitor, vor apărea elemente noi în identificarea unei persoane fizice.



UNIUNEA EUROPEANĂ



Pot fi prelucrate datele personale ale candidaților care au trimis CV-uri pentru un post? Cât timp? Trimiterea CV-ului poate fi considerată consimțământ pentru realizarea prelucrării datelor personale, dar numai în scopul pentru care CV-ul a fost trimis, adică în scop de recrutare. Datele personale astfel obținute nu pot fi însă utilizate pentru campanii de marketing, căci nu s-ar putea considera că trimiterea CV-ului are semnificația exprimării consimțământului. Publicarea fotografiei se face prin încărcarea fotografiei în sistem (art 9 alin. 1 lit. e)), adică datele (biometrice) sunt făcute publice în mod manifest de către persoana vizată. Datele se păstrează cât timp a dorit aplicantul, când și-a dat consimțământul.

In situatia unei afaceri care are ca obiect de activitate desfasurarea de cursuri si activitati pentru copii, tabere, este necesara desemnarea unui DPO?

Pentru a fi obligatoriu DPO este necesară întrunirea următoarelor condiții, în mod cumulativ:

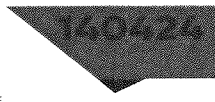
- Operațiunile de prelucrare necesită monitorizare periodică
- Operațiunile de prelucrare necesită monitorizare pe scară largă
- Operațiunile de prelucrare necesită monitorizare sistematică
- Operațiunile de prelucrare reprezintă o activitate principală a operatorului (prin natura, domeniul de aplicare și/sau scopurile operațiunilor) sau a următoarelor condiții, în mod cumulativ:
 - Operațiunile de prelucrare se referă la date speciale
 - Operațiunile de prelucrare reprezintă o activitate principală a operatorului (prin natura, domeniul de aplicare și/sau scopurile operațiunilor).

Ce documente, registre etc. trebuie întocmite în acest caz particular?

Întreaga activitate a operatorului ar trebui să fie atent procedurată, cu integrare atentă a dispozițiilor privind protecția datelor în procedurile de lucru existente sau chiar întocmirea de proceduri noi, acolo unde nu există. Verificarea procedurilor existente depinde de efectuarea auditului care se finalizează printrun raport ce asigură o imagine de ansamblu asupra situației operatorului de date cu caracter personal. Numai după efectuarea unui asemenea auditoperatorii vor putea ști concret care sunt pașii de urmat pentru finalizarea procedurilor și vor putea estima cu precizie durata și costurile.

Pozele pe care le facem la activitati copiilor pentru care avem acordul explicit din partea parintilor, pot fi postate pe rețelele personale de socializare, pe site?

Este nevoie de consimțământul expres din partea tuturor părinților copiilor care apar în poze. Fotografiiile reprezintă date biometrice, care, în speță, pot fi prelucrate au fost făcute publice în mod manifest de către persoanele vizate sau părinții lor, de exemplu în paginiile Facebook proprii. În caz contrar, este nevoie de consimțământul expres din partea părinților, consimțământ care, atenție, trebuie să fie granulat, adică să fie acordat pentru postarea pe pagina Facebook a





UNIUNEA EUROPEANĂ



companiei, nu și pe alte pagini. Cu alte cuvinte, trebuie să faceți setările corespunzătoare de privacy cu privire la aceste imagini.

Pozele în care apar copii, care exista deja din anii anteriori pe Facebook/site, pot ramane publicate?

Da, dacă aveți consimțământul expres din partea tuturor părinților copiilor care apar în poze și puteți face dovada acestui consimțământ. Realist vorbind, probabil că nu veți putea...

Ce clauze particulare trebuie introduse în contractele de prestari servicii educationale pe care le încheiem cu parintii, referitoare la aceste reglementari?

Clauze specifice privind protecția datelor care să reflecte măsurile tehnice și organizatorice luate în vederea asigurării unui nivel de securitate corespunzător (art. 32 din Regulament).

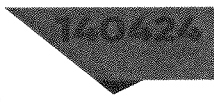
Microintreprinderile sunt obligate sau este optionala implementarea procedurilor impuse de legea privind GDPR.

Doar în sectorul public este obligatorie desemnarea unui responsabil, în mediul privat este o recomandare, obligativitatea fiind valabilă doar la operatorii care prelucrează date la scară largă. 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 (art. 4 pct. (7) RGPD). Cu alte cuvinte, operator este cel pentru care se realizează prelucrarea datelor, chiar dacă operatorul nu realizează el însuși nicio prelucrare (clienți sau salariați).

Regulamentul nu se aplică prelucrării datelor cu caracter personal:

- a) în cadrul unei activități care nu intră sub incidența dreptului Uniunii;
- b) de către statele membre atunci când desfășoară activități care intră sub incidența capitolului 2 al titlului V din Tratatul UE; (politica de securitate și apărare comună)
- c) de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice;
- d) de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor, sau al executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora.

Desemnarea DPO este doar una dintre măsurile instituite de Regulament....





UNIUNEA EUROPEANA



Pentru a fi obligatoriu DPO este necesară întrunirea următoarelor condiții, în mod cumulativ:

- Operațiunile de prelucrare necesită monitorizare periodică
- Operațiunile de prelucrare necesită monitorizare pe scară largă
- Operațiunile de prelucrare necesită monitorizare sistematică
- Operațiunile de prelucrare reprezintă o activitate principală a operatorului (prin natura, domeniul de aplicare și/sau scopurile operațiunilor) sau a următoarelor condiții, în mod cumulativ:
 - Operațiunile de prelucrare se referă la date speciale
 - Operațiunile de prelucrare reprezintă o activitate principală a operatorului (prin natura, domeniul de aplicare și/sau scopurile operațiunilor)

Ce obligatii vor avea contabilii in urmatoarele situatii: - sunt angajati cu CIM la una sau mai multe firme, si aici pot fi cu munca la domiciliu sau nu; - presteaza servicii ca liber profesionist in baza unui contract.

Contabilii salariați trebuie să respecte clauzele specifice protecției datelor cu caracter personal inserate în CIM, fișa postului, regulamentul intern ș.a., să respecte instrucțiunile scrise ale operatorului cu privire la prelucrarea datelor cu caracter personal, să ia la cunoștință de ele și să participe la programe de instruire în acest sens. Contabilii liber profesioniști sunt însă împuterniciți, și totodată operatori, dacă au salariați.

Ce obligatii au detinatorii camerelor de supraveghere?

Majoritatea organizatiilor realizează monitorizari video, și deci colectează datele cu caracter personal în scopul supravegherii activității salariaților și/sau în scop de pază. Deși dispozițiile art. 9 alin. 1 par să impună necesitatea consimțământului expres (Se interzice prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice.), lit. b), e) sau f) ar putea să justifice monitorizarea video, căci altminteri ar trebui să considerăm că Regulamentul impune ca monitorizarea video în scop de pază să fie făcută exclusiv pe bază de consimțământ expres a persoanelor care pătrund în incintă, ceea ce ar fi absurd.

În același sens, se va pune problema dacă monitorizarea video concretă pe care o companie o face se referă la “date biometrice pentru identificarea unică a unei persoane fizice”, căci este o mare diferență între autentificarea prin scanarea irisului sau amprentă și monitorizarea video cu rezoluție mică.





UNIUNEA EUROPEANĂ



Instrumente Structurale
2014-2020

În acest din urmă caz, imaginile obținute prin monitorizarea video este posibil să nu fie suficiente pentru identificarea unică a unei persoane fizice, ci doar dacă sunt corelate cu alte informații cu privire la salariați, numerele de înmatriculare ale autoturismelor care pătrund în incintă ș.a. În orice caz, nici obținerea consimțământului de la toate persoanele fizice care pătrund în incintă nu este o soluție, din pricina problemelor pe care le ridică obținerea consimțământului salariaților pentru monitorizarea video. Fără îndoială, un studiu de impact este necesar. Pe de altă parte, se impune o discuție cu privire la monitorizarea video care NU se face în scop de pază...

Avem obligația de a instiinta ANCOM, sub ce forma? ANSPDCP.

Nu. Dacă întrebarea se referă la monitorizarea video, atunci răspunsul este DA, întrucât evaluarea impactului asupra protecției datelor va indica faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri luate de operator pentru atenuarea riscului. Supravegherea video la locul de muncă prezintă risc ridicat.

10. Este recomandat unei companii (producție industrială) cu 300 salariați (a fost numit DPO) care decide instalarea unui sistem de supraveghere video efectuarea de DPIA?

Fără îndoială că DA, a se vedea răspunsul anterior.

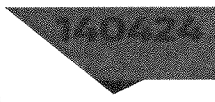
Bancile sunt persoane imputernicite sau terti în relația cu operatorul?

(operațiuni curente: plata salariilor, plăți către furnizori, încasări de la client, factoring, finanțare, linii de credit, etc). Sunt obligate să ne transmită acorduri/acte adiționale în privința protecției datelor? Băncile sunt operatori asociați. În cazul în care doi sau mai mulți operatori stabilesc în comun scopurile și mijloacele de prelucrare, aceștia sunt operatori asociați. Ei stabilesc într-un mod transparent responsabilitățile fiecăruia în ceea ce privește îndeplinirea obligațiilor care le revin în temeiul Regulamentului. În practică naște discuții raportul de forțe operator-împuternicit...

Cum se procedează cu Certificat naștere minori?

În unele cazuri (acordarea unor drepturi: deduceri personale sau beneficii la nașterea unui copil). Îl păstrăm la dosar? Certificatele de naștere ale copiilor salariaților ar trebui să fie depozitate și accesate sub autoritatea Serviciului Resurse Umane. În vederea respectării principiului reducerii prelucrării datelor cu caracter personal și pentru a restrânge accesul persoanelor la datele cu caracter personal, certificatele de naștere ale copiilor salariaților ar trebui depozitate sub cheie sub autoritatea Șefului de Serviciu.

Ce facem cu documentele (ex. caziere, formulare în care apare religia, poze, certificate de naștere ale copiilor, certificate de căsătorie, deces etc.) pe care le avem deja stocate (unele, dar nu toate, sau nu numai la dosarele personale).





UNIUNEA EUROPEANĂ



Instrumente Structurale
2014-2020

Ar trebui să fie depozitate și accesate sub autoritatea Serviciului Resurse Umane. În vederea respectării principiului reducerii prelucrării datelor cu caracter personal și pentru a restrânge accesul persoanelor la datele cu caracter personal, certificatele de naștere ale copiilor salariaților ar trebui depozitate sub cheie sub autoritatea Șefului de Serviciu.

In afara de cazul in care se produc incidentele de Securitate cand se mai notifica OBLIGATORIU autoritatea?

Operatorul sau persoana împuternicită de operator notifică măsurile luate în vederea respectării deciziei autorității de supraveghere. Operatorul consultă autoritatea de supraveghere înainte de prelucrarea atunci când evaluarea impactului asupra protecției datelor indică faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri luate de operator pentru atenuarea riscului (DPIA). Operatorul informează autoritatea de supraveghere cu privire la transfer. Operatorul sau persoana împuternicită de operator publică datele de contact ale responsabilului cu protecția datelor și le comunică autorității de supraveghere.

Este obligatoriu sa ne inscriem ca OPERATOR de prelucrare a datelor?

Nu.

Este necesara intocmirea unei baze de date separate cu toti clientii consumatori ai unei societati?

Operatorul trebuie să ia măsuri tehnice și organizatorice adecvate activității desfășurate. „Pseudonimizare” înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separate și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile (art. 4 pct. 5 RGPD).

Este voie sa numim printr-o decizie al Administratorului societatii un angajat al societatii responsabil cu protectia datelor?

Da.

18. Responsabilul cu protectia datelor este obligat sa participe la un curs de specializare?

Nu, nu este obligatoriu, poate să studieze singur.



UNIUNEA EUROPEANA



Este obligatoriu sa trimitem clientilor consumatori ai societatii o instiintare referitoare la scopul prelucrării datelor?

Simpla preocupare pentru protecția datelor cu caracter personal ("informarea generala") nu este suficientă pentru respectarea prevederilor GDPR. Scopul Regulamentului este acela de a determina operatorii să își adapteze procesele interne și relațiile cu alții (furnizori, beneficiari, poprii salariați), să adopte măsuri organizatorice speciale și să implementeze proceduri de securitate adecvate, toate acestea pentru a asigura protecția datelor cu caracter personal. Da, informarea persoanelor vizate este obligatorie, însă nu este suficientă.

O societate comerciala ce desfasoara activitate de comert ambulant, fara salariatii, este obligata sa se inregistreze ca operator de date cu caracter personal, daca aceste date cu care intra in contact se folosesc doar pentru desfasurarea activitatii (emitere facturi fiscale, incheiere contracte comerciale)?

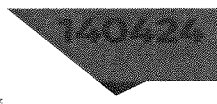
Datele cu caracter personal sunt stocate in programul de facturare. Nu este necesara înregistrarea ca operator de date, însă reglementările privind protecția datelor din Regulament sunt pe deplin aplicabile.

O societate comerciala care desfasoara activitate de comert online, cu salariatii, este obligata sa se inregistreze ca operator de date cu caracter personal daca aceste date se folosesc doar pentru emiterea de facturi, contracte comerciale, intocmire oferte de pret la solicitarea potentialilor clienti, intocmire contracte individuale de munca?

Datele cu caracter personal se stocheaza in programul de facturare si salarizare. Nu este necesara înregistrarea ca operator de date, însă reglementările privind protecția datelor din Regulament sunt pe deplin aplicabile.

O societate comerciala, in calitate de Prestator, care incheie contract de prestari servicii secretariat cu o alta companie, este obligata sa se inregistreze ca operator de date cu caracter personal, avand in vedere ca intra in contact cu datele personale ale clientilor beneficiarului? (aceste servicii de secretariat desfasuranduse la sediul Beneficiarului). In ce consta procedura GDPR pentru o astfel de societate?

Nu este necesara înregistrarea ca operator de date, însă reglementările privind protecția datelor din Regulament sunt pe deplin aplicabile. Operatorii de date personale au posibilitatea să apeleze la alte persoane, pe care să le împuternicească să realizeze prelucrarea datelor cu caracter personal. Activitatea privind protecția datelor cu caracter personal poate fi, de asemenea, exercitată în baza unui contract de prestări servicii încheiat cu o persoană fizică sau o organizație din afara organizației operatorului/persoanei împuternicite de operator.





UNIUNEA EUROPEANĂ



Dar desemnarea unui reprezentant de către operator sau a unei persoane împuternicite de operator nu aduce atingere acțiunilor în justiție care ar putea fi introduse împotriva operatorului sau persoanei împuternicite de operator... Nu doar persoanele vizate, ci și autoritatea de supraveghere se pot adresa și direct operatorului, cu privire la toate chestiunile legate de prelucrarea datelor.

Procedura pentru fiecare department in parte cuprinde exact datele cu caracter personal care se prelucreaza, de unde provin si trasabilitatea?

Da. Procedura pentru fiecare departament trebuie să cuprindă cel puțin informații cu privire la întocmirea, primirea, păstrarea, accesarea, transmiterea, transportul, utilizarea și predarea documentelor care conțin date cu caracter personal.

Cartografierea se face pe fiecare departament in parte si pe fiecare punct de lucru?

Da. Mai mult decât atât, ar fi recomandat să se facă pe fiecare document care conține date cu caracter personal, precum și transversal (date cu caracter personal care trec de la un departament la altul).

Cum se face instruirea salariaților, prin luarea la cunostința a procedurilor fiecărui departament in parte?

Modalitatea de instruire a salariaților depinde de specificul activității Operatorului și de modul cum înțelege să realizeze acest lucru. Este recomandat să se organizeze și sesiuni de instruire a salariaților care lucrează cu informații care conțin date cu caracter personal. Aducerea la cunoștință a procedurilor fiecărui departament este subînțeleasă.

Adaptarea contractelor de vanzare cu clientii la noile cerinte se face prin act aditional, informare?

Act adițional care să conțină dispoziții speciale privind protecția datelor cu caracter personal, precum și prin nota de informare. Dacă vizați utilizarea datelor colectate cu ocazia contractelor în scop de marketing, atunci trebuie să obțineți în mod granulat consimțământul, adică distinct pentru fiecare scop al prelucrării.

In cazul unuiu magazin online care comercializeaza ingrediente cosmetice, este necesar sa cerem consimtamantul clientilor pentru a le trimite emailul de confirmare a comenzii si copia facturii, sau doar pentru a le trimite newsletterul-ul?

Cele două prelucrări (confirmarea comenzii + transmiterea facturii fiscale și transmiterea newsletterului) au temeuri juridice de prelucrare diferite (art. 6 alin. (1) GDPR), respectiv:



UNIUNEA EUROPEANĂ



a) persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice (newsletterul).

b) 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 (confirmarea comenzii și transmiterea facturii fiscale). Prin urmare, dacă prelucrarea se efectuează pe baza unui alt temei juridic (pct. b), nu este necesar consimțământul.

Nu îi lasam să acceseze site-ul dacă nu își dau consimțământul pentru google analytics / cookie servicii externe?

În cazul în care prelucrarea se bazează pe consimțământ, operatorul trebuie să fie în măsură să demonstreze că persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal. Consimțământul trebuie dat în mod liber.

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

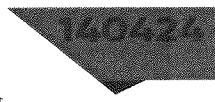
Regulamentul vizează toate societățile juridice, indiferent de cifra de afaceri sau numărul de utilizatori?

Apropie toate, 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 (art. 4 pct. (7) RGPD).

Datele referitoare la starea de sănătate sunt preluate pentru ca angajatorul să cunoască aceste aspecte cu privire la angajații care prezintă anumite probleme de sănătate.

În funcție de aceste date, șefii ierarhici superiori, cunosc modul în care un angajat cu anumite probleme de sănătate poate să lucreze sau nu în schimb de noapte. Așadar, aceste date sunt preluate, colectate de către Dep. HR, dar ele sunt cunoscute și de alte persoane din cadrul firmei (ex. șefi ierarhici superiori). Pentru a proteja datele în acest caz, este suficient să încheiem acte adiționale privind confidențialitatea și secretul datelor cu caracter personal, cu acei șefi ierarhici superiori?

Salariații care urmează să desfășoare munca de noapte sunt supuși unui examen medical gratuit înainte de începerea activității și, după aceea, periodic (art. 127 alin. (1) din Codul Muncii). Șefii ierarhici trebuie să cunoască dacă subordonații sunt apti sau nu pentru munca de noapte, nu și problemele de sănătate. Toți salariații care prelucrează date cu caracter personal trebuie să aibă în fișa postului dispoziții cu privire la respectarea protecției datelor cu caracter personal.





UNIUNEA EUROPEANĂ



Cum protejăm datele cu caracter personal despre care luăm la cunoștință de pe facturile transmise societății noastre?

Sau cele cuprinse în contractele de vânzare cumpărare pe care în mod uzual le încheiem. Pe aceste documente apar date personale cum ar fi: nume, Prenume, uneori CNP. Prin măsuri tehnice și organizatorice luate în vederea asigurării unui nivel de securitate corespunzător.

Cum protejăm datele personale identificate în semnătura din mail-uri transmise sau primite? (nume, Prenume, funcție, telefon/fax).

Prin măsuri tehnice și organizatorice luate în vederea asigurării unui nivel de securitate corespunzător.

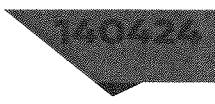
Există un text tip care trebuie semnat/acceptat ca și consimțământ?

Nu există un text tip. Aceasta întrucât la momentul luării consimțământului trebuie specificat expres care este scopul prelucrării de date cu caracter personal, acest scop putând varia de la caz la caz. Condițiile cu privire la modalitatea în care consimțământul trebuie exprimat, respectiv, obținut sunt prevăzute în art. 7 din Regulament. Se poate concepe un text predefinit în cazul în care operatorul se limitează doar la prelucrarea anumitor date într-un scop sau mai multe scopuri determinate, însă în cazul în care se modifică scopul prelucrării este necesar ca regulă includerea acestui nou scop în cadrul acordului de exprimare a consimțământului.

Prin cookies se pot colecta date cu caracter personal? Este folosirea de cookies încadrată în prelucrarea de date cu caracter personal?

Persoanele fizice pot fi asociate cu identificatorii cookie (Considerentul 30 din Regulament). Aceștia pot lăsa urme care, în special atunci când sunt combinate cu identificatori unici și alte informații primite de servere, pot fi utilizate pentru crearea de profiluri (= prelucrare automată a datelor cu caracter personal – art. 4 pct. 4 fin Regulament) ale persoanelor fizice și pentru identificarea lor. Prin identificatorii cookie pot fi colectate date cu caracter personal, chestiune ce depinde de tipul acestora: per sesiune, de persistență, de localizare etc.

Prin „prelucrare” se înțelege orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea (art. 4 pct. 2 din Regulament). Astfel, în situația în care cooki-urile pot ajuta la identificarea unui dispozitiv folosit pentru conectare, respectiv, a utilizatorului, în combinație cu alte elemente, în contextul înregistrării informațiilor obținute prin intermediul lor, putem fi în prezența unei prelucrări de date cu caracter personal.





UNIUNEA EUROPEANĂ



Cum putem face dovada distrugerii efective a informațiilor arhivate în calculatoare, fără să distrugem hard-ul?

O variantă de dovedire a responsabilității ar fi înregistrarea acțiunii de ștergere/a formatării lui sau pe baza eventualelor înregistrări la nivelul sistemului de operare. Situațiile în care ca datele cu caracter personal șterse, fără nicio intenție din partea operatorului de a le utiliza sau de a le accesa din nou, există în continuare în sistemul electronic pot fi multiple. De exemplu, datele ar putea aștepta să fie suprascrise cu alte date.

Deși poate fi posibil să se reconstituie informația din bucățile de hârtie, acest lucru ar fi extrem de dificil și este puțin probabil ca organizația să aibă intenția să facă acest lucru). Astfel, se poate întâmpla ca ștergerea, chiar și „permanentă” a datelor cu caracter personal de pe un Hard Disk să nu asigure ștergerea definitivă a lor, întrucât informații parțiale vor continua să fie stocate și ulterior, acestea putând fi chiar restaurate prin aplicarea unor proceduri speciale. De aceea, se recomandă apelarea la servicii IT de specialitate în vederea conformării activităților cu prevederile GDPR. Ulterior unei astfel de ștergeri definitive a datelor, Autoritatea de Supraveghere națională poate să procedeze la verificarea dispozitivelor pentru a constata faptul că nu se mai dețin datele șterse.

Ce obligație revine celui care folosește newsletter-ul ca modalitate de informare?

Obligația de a obține consimțământul utilizatorilor cu privire la primirea în continuare de newsletter, precum și posibilitatea de și-l retrage oricând.

Ce măsuri de securitate fizică sunt necesare pentru protecția serverelor, din perspectiva GDPR?

Amplasarea acestora într-o zonă ferită de dezastre. Și recomandabil ar fi să existe un al doilea rând de servere care pot prelua activitatea serverului principal în caz de dezastru sau inactivitate. De asemenea, în locația în care sunt amplasate serverele, ar trebui să fie instituite și implementate proceduri bine puse la punct în caz de seism, incendiu etc. O altă variantă ar fi plasarea serverelor în Cloud împreună cu pasarea parțială a responsabilității către furnizorul de servicii.

În cazul unei instituții publice care prelucrează deja date cu caracter personal, mai este nevoie să notifice autoritatea?

Odată cu intrarea în vigoare a Regulamentului 679/2016 a fost eliminată necesitatea notificării Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal. Astfel că la acest moment, atât persoanele juridice private cât și cele publice nu mai au această obligație. O instituție publică este obligată să își desemneze un Responsabil cu protecția datelor cu caracter personal (DPO), iar datele de contact ale acestuia trebuie comunicate Autorității.