

Cuprins

GDPR-UL DIN PUNCTUL DE VEDERE AL AFACERILOR (COMPANIILOR/SOCIETĂȚILOR) – IMPACTUL ECONOMIC ȘI ORGANIZAȚIONAL.....	13
BUNE PRATICI ÎN MANAGEMENTUL ȘI ADMINISTRAREA COMPANIEI.....	28
Implementarea clauzelor GDPR în actul constitutiv al firmei și în AGA.....	28
Adunarea Generală a Asociațiilor.....	31
Implicarea administratorului în luarea măsurilor tehnice și organizatorice și în monitorizarea lor. Numirea unui DPO/DPC	32
Monitorizarea măsurilor tehnice și organizatorice	35
Cooperarea între administrația societății și DPO/DPC.....	36
GDPR și controalele de la autoritățile publice. Registrul unic de control	38
Registrul unic de control	40
Asigurarea implementării GDPR la punctele de acces în societate. Recepția și poarta	41
Procedura de acces în companie	41
Supravegherea video	44
Verificarea identității prin sisteme tehnice și imagini	48
Alte date prelucrate la punctele de acces	52
Puncte de recepție multi-task	53
Stabilirea fluxului de date cu caracter personal în societate	54
Registrul de prelucrare	58
Modificări legislative și impactul în activitatea de prelucrare.....	60
Arhivarea sau distrugerea documentelor care conțin date cu caracter personal	62
Principii generale	62
Elementele principale înregistrate de companii.....	63
Suportul de arhivare	65
Persoanele desemnate.....	66
BUNE PRACTICI ÎN DEPARTAMENTELE JURIDIC, FINANCIAR ȘI DE RESURSE UMANE	68
Aplicarea GDPR în departamentul juridic. Bune practici.....	69
Scopurile prelucrării	69

Temeiurile de prelucrare la nivelul departamentului juridic	70
Responsabilitățile personalului din departament	71
Procedura de soluționare a cererilor și a plângerilor	73
Procedura soluționării plângerilor împotriva răspunsului la o cerere	76
Registrul GDPR pentru contracte	78
Proceduri recomandate pentru conformarea cu GDPR	
a departamentului financiar/contabil. Bune practici	81
Fluxul operațional al prelucrării datelor cu caracter personal	82
Procedură pentru decontarea sumelor pentru concediile medicale	82
Întocmirea documentelor pentru încasări și plăți. Facturarea	84
Procedura de prelucrare a datelor cu caracter personal în cadrul gestionării procesului de recuperare a creanțelor	86
Tipurile de date colectate în departamentul financiar-contabil. Particularități și exemple	88
Date prelucrate de departamentul financiar contabil	88
Înmânarea fluturașilor de salariu	88
Acordarea tichetelor de masă	89
Decontarea cheltuielilor pentru deplasări	90
Proceduri recomandate pentru conformarea cu GDPR	
a departamentului de HR. Bune practici	92
Tipuri de activități desfășurate de departamentul resurse umane	93
Tipuri de date cu caracter personal prelucrate de departamentul de resurse umane	93
Prelucrarea de date în faza de recrutare. Particularități	94
Despre prelucrarea datelor din cazierul judiciar	95
Legitimațiile de serviciu, pontajele și permisele de parcare	97
Prelucrarea datelor cu caracter personal privind confesiunea religioasă	101
Prelucrarea imaginilor salariaților prin foto/video	102
Monitorizarea video a angajaților care utilizează mijloace de transport în comun puse la dispoziție de angajator	102
Camerele supraveghere amplasate în incinta de lucru a angajaților	103
Publicarea fotografiilor și videoclipurilor de la activitățile individuale sau colective profesionale și extra-profesionale	104
Administrarea dosarelor de personal. Tipuri de date prelucrate. Bune practici	107
Eliberarea adeverințelor care atestă corectitudinea datelor. Scrisori de recomandare	109

Prelucrarea datelor în timpul unei cercetări disciplinare.....	111
Mijloacele de comunicare utilizare cu și de către salariați	112
BUNE PRACTICI ÎN DEPARTAMENTELE DE MARKETING, VÂNZĂRI ȘI CLIENT SUPPORT.....	114
Departamentul de Marketing	114
Descrierea activităților de marketing la nivel intern.....	116
Scopurile prelucrării datelor cu caracter personal în departamentul de marketing.....	117
Legalitatea prelucrării datelor cu caracter personal (temeiuri legale) de către departamentul de marketing.....	118
Prelucrarea se bazează pe consimțământul persoanei vizate.....	119
Condițiile pe care trebuie să le îndeplinească consimțământul	120
Pentru ce perioadă se acordă consimțământul?	124
Retragerea consimțământului.....	125
Consimțământul copiilor	127
Bune practici privind obținerea consimțământului	129
Prelucrarea se bazează pe un interes legitim	132
Activități specifice Departamentului de Marketing în contextul GDPR	134
Site-ul societății. Bune Practici	134
Politica de confidențialitate	137
Cookie-uri. Politica de cookies a site-ului companiei	139
Profilarea, un instrument de marketing din ce în ce mai des folosit de către companii.....	142
Organizarea de concursuri și campanii promoționale	146
Promovarea produselor pe rețelele de socializare	148
Abonarea la newsletter.....	148
Publicarea articolelor de presă	149
Bune practici privind aplicarea GDPR-ului în domeniul Marketing	150
Departamentul de Vânzări.....	151
Datele cu caracter personal prelucrate care se prelucrează de către Departamentul de Vânzări.....	152
Temeiurile prelucrării datelor cu caracter personal	153
Bune practici ale Departamentului de Vânzări în domeniul datelor cu caracter personal	154
Departamentul de Client Support	155
Datele cu caracter personal prelucrate care se prelucrează de către Departamentul de Client Support	156
Temeiul prelucrării datelor cu caracter personal	156

Bune practici ale Departamentului de Client Support în domeniul datelor cu caracter personal	156
Informarea persoanelor vizate asupra drepturilor pe care acestea le au	157
MĂSURI TEHNICE ȘI ORGANIZATORICE	161
Responsabilitatea operatorului. Privacy by design & by default.....	161
Măsuri tehnice	166
Securizarea echipamentelor prin intermediul cărora se prelucrează date cu caracter personal	168
Autentificarea unică a membrilor personalului.....	168
Executarea copiilor de siguranță	170
Anticiparea incidentelor de securitate ce ar putea rezulta din pierderea sau furtul unui echipament	170
Securizarea serverelor.....	171
Protejarea rețelei interne de internet	172
ISO27 001:2013.....	172
Măsuri organizatorice	173
Planul de conformare.....	173
DPO-ul	175
Evidența activităților de prelucrare	177
Analiza interesului legitim	185
Instruirea salariaților	186
Limitarea accesului	191
Politici și proceduri.....	192
Politica privind exercitarea drepturilor persoanelor vizate.....	195
Dreptul de acces la date	195
Dreptul la rectificare.....	197
Dreptul de a fi uitat.....	197
Dreptul la restricționarea prelucrării.....	198
Dreptul la portabilitate.....	199
Dreptul la opoziție	200
Dreptul de a nu face obiectul unei decizii automate.....	200
Dreptul la retragerea consimțământului.....	201
Dreptul de a formula o plângere la autoritatea de supraveghere	201
Dreptul de a se adresa instanțelor de judecată	203
Politica privind retenția datelor	203
Procedura pentru incidente de securitate.....	206
Evaluarea partenerilor comerciali	209
Notele de informare	209

Informarea salariaților și a aplicanților pentru un post disponibil în cadrul companiei	210
Informarea partenerilor/clientilor	211
Informarea vizitatorilor	211
Consultarea reprezentanților angajaților cu privire la sisteme ce presupun prelucrări de date în spațiile în care se desfășoară activitate	212
Acordurile privind protecția datelor cu caracter personal	214
Auditul intern	217
Auditul preliminar	217
Raportul de audit	218
PRACTICA AUTORITĂȚILOR	220
Clasamentul sancțiunilor prin raportare la încălcări	222
Clasamentul sancțiunilor prin raportare la cuantumul amenzilor	222
Clasamentul sancțiunilor prin raportare la numărul amenzilor	223
Analiza măsurilor dispuse de autoritățile de supraveghere	223
Austria	223
Belgia	226
Bulgaria	231
Croația	237
Cipru	238
Cehia	240
Danemarca	243
Estonia	245
Finlanda	246
Franța	247
Germania	249
Grecia	259
Italia	263
Letonia	269
Lituania	270
Malta	270
Olanda	271
Polonia	273
Portugalia	276
România	277
Slovacia	287
Spania	289
Suedia	294

Ungaria	297
Modalitatea prin intermediul căreia este inițiată o investigație	309
Controlul efectuat de ANSPDCP este întotdeauna anunțat?	311
Pot amâna efectuarea unei investigații anunțate?	312
Desfășurarea efectivă a procedurii investigației	313
Efectuarea investigațiilor pe teren	314
Efectuarea investigațiilor la sediul ANSPDCP	316
Efectuarea investigațiilor în scris	316
Aspecte particulare privind investigațiile desfășurate la autoritățile/organismele publice	318
Procesul-verbal încheiat de ANSPDCP. Elemente componente. Căi de atac. Posibile sancțiuni.....	319

Prefață

Înainte de prefața cărții vreau să vorbesc despre „a scrie în ziua de azi”. Cine mai are nevoie de informații din cărți în epoca platformelor și vitezei, cine mai are timp să citească atunci când ar putea să ia concluziile gândite de alții deja și, pe scurt, oare ce le motivează pe tinerele autoare să scrie?

Nu e mai ușor să plătești publicitate sau să vorbești la o emisiune TV?

Cred că a scrie este o obligație a oricărui intelectual care lucrează cu concepte – atunci când scrii nu ai doar dreptul de exprimare, dar și obligația de a fi consistent. Atunci când scrii și recitești ești și arhitect, și constructor, dar și consumator de idei, altfel nu poți depăși o pagină sau două. Într-o epocă a volumului și vorbitului, este nevoie de mai multă responsabilitate și, înainte de toate, este nevoie să vedem scrisul ca pe o lucrare personală, ca o parte din moștenirea pe care o minte scripitoare trebuie să se asigure că o transmite și altora, că o împarte cu cititorii.

Trecând mai departe, tema cărții este provocatoare – dreptul ca disciplină este un dinozaur viu, pentru că legile sunt pentru și despre oameni și societăți. Cu fiecare carte scrisă despre legi și despre modul cum funcționăm se clădește o conștiință colectivă a ceea ce înseamnă societate, reguli, ce este acceptabil, despre bine și rău. Pe lângă interes, cartea de față este o lucrare folositoare și întărește nu doar obligația de a scrie, dar și obligația de a interpreta și provoca principiile vechi la noile realități.

Sunt legi și principii vechi de mii de ani, care încă stau la baza relațiilor noastre, și există și legi noi pentru provocări noi – cum este GDPR, consecința avântului globalizării și tehnologizării din viața fiecărui om.

Interesant pentru mine este că citatul din începutul cărții pune legislația GDPR sub semnul vechii bătălii din Lumea Nouă și Bătrânul Continent, aducând demnitatea în centrul societății, ca o valoare esențială a ființei umane. Sunt idei umaniste cărora în sfârșit le-a venit vremea. Eliberat de foame și sclavie sub diferite forme, omul de rând își caută sensul și limitele libertății.

Libertatea de a înțelege ce se întâmplă cu informațiile despre tine, libertatea de a-ți administra opțiunile personale, precum și multe altele detaliate în prezenta carte sunt de fapt o digitalizare a relațiilor omenești în care ideile sunt noile valori și cursa este despre a înțelege opțiunea

maselor. Deciziile în timp real impun reguli în timp real care să reechilibreze balanța de putere între algoritmi și oameni. Legile referitoare la protecția datelor vin să așeze lucrurile în societate și tocmai de aceea acest subiect este nu doar actual, dar mai ales relevant în viitor. Tehnologia și inteligența artificială avansează exponențial. E timpul ca oamenii să înțeleagă cine folosește informațiile, cum arată noua media, de ce personalizarea vine cu prețul viziunii și pentru cine implementăm de fapt GDPR.

Este o mare bucurie și onoare să fiu o mică parte din această lucrare care încearcă să ne aducă mai aproape legile și regulile – care ni se aplică, indiferent dacă le înțelegem sau nu. De fapt, cartea este un exercițiu de (auto)educație și tocmai de aceea vă felicit că o aveți în brațe și vă urez lectură plăcută!

Monica CADOGAN
CEO și fondator Vivre

GDPR-UL DIN PUNCTUL DE VEDERE AL AFACERILOR (COMPANIILOR/SOCIETĂȚILOR) – IMPACTUL ECONOMIC ȘI ORGANIZAȚIONAL

„A fi european înseamnă a avea dreptul ca datele tale cu caracter personal să fie protejate de legi puternice, europene. Pentru că europenilor nu le plac dronele care zboară pe deasupra lor și le înregistrează fiecare mișcare, nici companiile care contabilizează fiecare click pe mouse. De aceea, Parlamentul, Consiliul și Comisia au convenit în mai anul acesta un regulament comun privind protecția datelor cu caracter personal. Acest regulament este o lege europeană fermă aplicabilă companiilor, indiferent de locul în care își au sediul și ori de câte ori prelucrează datele dumneavoastră cu caracter personal. Pentru că, în Europa, păstrarea confidențialității datelor personale contează. Această chestiune ține de demnitatea umană”.

Jean Claude Juncker

Tuturor ne place să măsurăm – fie că vorbim despre profit, cifra de afaceri, marjă sau alți indicatori – ne place să raportăm și să ne raportăm la cifre. În cazul apariției GDPR-ului cei mai mulți s-au raportat la cât business s-a pierdut din cauza apariției Regulamentului European, câți bani s-au cheltuit pe consultanți, cât timp s-a pierdut pentru a răspunde la chestionare și câțiva s-au raportat la ce amenzi au avut de plătit.

Mai puțini s-au gândit la ce a însemnat pentru organizația lor implementarea unor reguli pentru a respecta GDPR-ul, schimbarea organigramei uneori chiar și a culturii organizaționale.

Foarte puțini oameni de afaceri s-au gândit la partea bună a lucrurilor, la securitatea sporită a datelor și a businessului implicit care a venit o dată cu implementarea GDPR-ului.

Noi, autoarele, ne propunem să explicăm pe înțelesul neprofesioniștilor ce trebuie să întreprindă o societate pentru a se conforma prevederilor GDPR. Astfel, fie că sunteți juristul din cadrul unei societăți, fie că lucrați în departamentul de Marketing sau Resurse Umane, fie că sunteți chiar administratorul societății, ne dorim ca această carte să fie un punct de sprijin pentru călătoria de conformare. Deși se spune că se poate

preciza cu exactitate momentul începerii implementării, dar niciodată nu se va ști când se va finaliza, GDPR-ul fiind un domeniu în care trebuie menținută atenția și concentrarea pe toată durata de viață a societății, ne propunem ca limbajul să fie unul accesibil (să ieșim din zona de „pășă-rească” a specialiștilor), astfel încât să putem sprijini cât mai multe persoane dornice să înțeleagă GDPR-ul. Cartea nu se dorește a fi una exhaustivă, dedicată specialiștilor, ci este una practică, cu multe exemple din experiența noastră, a autoarelor – care practică avocatura de afaceri, concentrându-se inclusiv pe protecția datelor, de mai bine de 17 ani.

După cum se știe, datele au valoare pecuniară. Având valoare financiară, ele se comercializează pe piață. Fac obiectul intermediarilor și al unui comerț intens. Analytics, big data, market profiling, inteligența artificială (AI), blockchain, IoT (internet-of-things) etc. – sunt doar câteva domenii notorii și prezente pe piața digitală.

Toate domeniile economiei și finanțelor în activitatea curentă, gestionează baze masive de date (banking, asigurări, servicii medicale private, contabilitate etc.) și își construiesc strategiile pe baza unor intense și din ce în ce mai sofisticate operațiuni de profilare și prelucrare a datelor personale.

Datelor personale le este recunoscută valoarea comercială în mod explicit inclusiv prin Directiva privind Contractele de furnizare de conținut digital și de servicii digitale din 26 martie 2019 (ce va trebui transpusă în legislația națională până la 01.07.2021), recunoscându-se datelor personale valoare de piață, prin care se achită un serviciu: „*Prezenta directivă se aplică și atunci când comerciantul furnizează sau se angajează să furnizeze consumatorului conținut digital sau un serviciu digital, iar consumatorul furnizează sau se angajează să furnizeze comerciantului date cu caracter personal (...)*”. Monetizarea, inclusiv pe cale legislativă a valorii datelor personale, este o realitate juridică.

Dar nu doar societățile din domeniul tehnologiei folosesc baze de date – datele cu caracter personal ale clienților sunt folosite de clinici, grădinițe și școli, magazine online, agenții de turism și recrutare etc., dar toate societățile dețin date cu caracter personal ale angajaților.

Deși se discută atât de mult de General Data Protection Regulation – (Regulamentul General privind Protecția Datelor), se pare că doar o parte din companiile europene au implementat obligațiile GDPR (cifrele diferă în funcție de sursă – mai puțin de jumătate, conform IAPP (International Association of Privacy Professionals) sau două companii din trei, conform unui studiu realizat de RSM pentru European Business Awards¹.

¹ <https://www.rsm.global/news/30-european-businesses-are-still-not-compliant-gdpr>.

De asemenea, se discută foarte mult de cât costă implementarea normelor GDPR – conform International Association of Privacy Professionals (IAPP), cele mai bogate 500 firme au cheltuit 7.8 miliarde de dolari pe implementarea GDPR, bugetul mediu pentru fiecare firmă fiind de 16.000.000 \$. Pe de altă parte, autoritățile naționale (inclusiv Comisia Europeană) insistă pe faptul că nu ar trebui cheltuite sume foarte mari, ci doar respectate normele impuse de GDPR, pornind de la principiile enumerate în preambulul regulamentului.

Este evident că investiția în soluțiile de securitate pentru criptarea datelor, asigurarea confidențialității, detectarea posibilelor amenințări, gestionarea răspunsurilor către persoanele vizate și mai ales pregătirea permanentă a angajaților presupune costuri, existând soluții scumpe și soluții ieftine, procese acoperitoare și dosare cumpărate „de-a gata” fără a fi implementate.

În ciuda costurilor, majoritatea companiilor au considerat că implementarea GDPR nu a dăunat dezvoltării lor – 65% dintre respondenți au considerat că GDPR a avut un impact pozitiv asupra afacerii lor și doar 15% au considerat că GDPR a avut un impact negativ asupra activității lor.²

La împlinirea unui an de la aplicarea GDPR, Comisia Europeană a publicat un raport conform căruia 67% dintre europeni au auzit de GDPR, în timp ce 57% dintre aceștia știu de existența unei autorități publice în fiecare țară care se ocupă de protejarea drepturilor lor în ceea ce privește datele cu caracter personal și către care pot trimite plângeri pentru încălcarea acestor drepturi.³

Chiar și în momentul pandemiei – o perioadă dificilă pentru toate statele lumii, în Europa nu s-a oprit discuția despre GDPR și despre importanța datelor cu caracter personal – fie că vorbim despre date de sănătate (temperatură), fie că vorbim despre numele persoanelor infectate sau despre localizarea lor exactă. De asemenea, societățile au trebuit să își completeze politicile privind prelucrarea datelor cu caracter personal pentru cazurile în care angajații aveau anumite boli cronice care ar fi presupus o precauție suplimentară.

Ce este GDPR?

GDPR reprezintă Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor

² GDPR Compliance Status TrustArc https://info.trustarc.com/Web-Resource-2018-07-12-GDPR-ResearchReport_TYP.html.

³ https://ec.europa.eu/info/sites/info/files/infographic-gdpr_in_numbers.pdf.

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).⁴ GDPR a fost publicat în Jurnalul Oficial al Uniunii Europene L119/4 mai 2016, a intrat în vigoare la 25 mai 2016 și este aplicabil din 25 mai 2018 la nivelul întregii Uniuni Europene.

GDPR nu reprezintă o noutate absolută, fiind de fapt doar o adaptare a Directivei 95/46/CE la modificările tehnologice și cerințele sporite privind securitatea datelor cu caracter personal.

Se vorbește de schimbări extraordinare, unii numesc o revoluție în domeniul protecției datelor – noi vrem doar să punctăm noutățile din domeniul protecției datelor cu caracter personal, subliniind faptul că GDPR:

- sporește drepturile individuale ale persoanelor vizate de colectarea și prelucrarea datelor cu caracter personal;
- lărgeste spectrul categoriilor de date cu caracter personal;
- impune noi obligații operatorilor de date cu caracter personal, precum și persoanelor împuternicite de aceștia, obligații care cu un impact tehnic și organizațional;
- stabilește amenzi semnificative în caz de neconformitate;
- impune în unele cazuri numirea unui DPO (Data Protection Officer – Responsabil de date cu caracter personal), persoană care trebuie să se asigure de aplicarea coerentă a dispozițiilor legale pentru a da eficiență acestora față de persoanele vizate.

Regulamentul este inclus în categoria documentelor care formează Cadrul european în domeniul securității cibernetice alături de alte trei documente (Convenția privind criminalitatea informatică, Directiva privind măsurile pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice și Strategia de securitate cibernetică a Uniunii Europene).

Acest regulament a influențat și alte legislații naționale, fiind un model pentru Brazilia, Japonia, China, Rusia și California. În Statele Unite, California a fost primul stat cu o mai bună protecție a datelor pentru cetățenii săi. În ceea ce privește forma și conținutul, acest Act de confidențialitate a consumatorilor din California (CCPA)⁵ este în mod clar comparabil cu GDPR european. De asemenea, în aprilie 2016, Republica Turcia a publicat Legea privind protecția datelor cu caracter personal w.

„Data protection by design” și „data protection by default”.

⁴ <http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016R0679>.

⁵ The California Consumer Privacy Act (CCPA) a intrat în vigoare pe 01.01.2020.

nr. 6698, în Monitorul Oficial. La cererea reprezentanților afacerilor turce, termenul pentru această înregistrare a fost amânat pentru 30.06.2020 când autoritatea turcă va putea începe amendarea celor care nu s-au conformat.

Cerut cu insistență de asociațiile de consumatori, scopul a fost acela de a proteja persoanele fizice, mai ales în contextul în care marile corporații au folosit și o parte din ele încă folosesc datele personale în moduri greu de înțeles pentru persoanele obișnuite, precum și pentru a determina companiile să acorde o atenție mai mare protecției datelor.

„Unul dintre principalele scopuri ale Regulamentului general privind protecția datelor este de a da mai multă putere oamenilor și de a le oferi mai mult control asupra uneia dintre cele mai valoroase resurse din economia modernă – datele lor. Putem atinge acest obiectiv numai dacă și când oamenii devin pe deplin conștienți de drepturile lor și de consecințele deciziilor lor.

Începem deja să vedem efectele pozitive ale noilor reguli. Cetățenii au devenit mai conștienți de importanța protecției datelor și a drepturilor lor. Și acum își exercită aceste drepturi, așa cum realizează autoritățile naționale de protecție a datelor în activitatea lor de zi cu zi. Au primit până acum peste 95.000 de reclamații din partea cetățenilor.” (Declarație comună a Vice-Președintelui Timmermans, Vice-Președintelui Ansip, Comisarului European Jourová and Gabriel, cu ocazia Zilei Internaționale a Datelor cu caracter personal, 25.01.2019)

Ce sunt datele cu caracter personal?

„Datele cu caracter personal” au fost definite în cadrul Regulamentului ca fiind „orice informații privind o persoană fizică identificată sau identificabilă („persoană 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;”

Foarte important de reținut este faptul că datele personale nu se limitează la elemente ușor de înțeles precum CNP-ul, adresă, nume, adresa de email etc., ci aria este mult mai extinsă în noul regulament, cuprinzând și informații legate de localizarea prin GPS, adrese IP, asigurări, date părinți și copii, date biometrice, datele referitoare la preferințele de cumpărare, religie, sex, etnie sau locul de muncă.

Exemple de date care nu sunt considerate a fi date cu caracter personal:

- CUI-ul/CIF-ul unei societăți;
- O adresă de e-mail care are formatul info@numecompanie.com, secretariat@numecompanie.ro, vanzari@numecompanie.eu;
- Sediul unei societăți;
- Datele anonimizate;
- Numărul de telefon al unei societăți publicat pe pagina sa web.

Normele GDPR se aplică numai datelor cu caracter personal privind persoanele fizice și nu reglementează datele referitoare la societăți sau la alte entități juridice.



Atenție! Cu toate acestea, informațiile legate de societăți alcătuite dintr-o singură persoană pot constitui date cu caracter personal dacă permit identificarea unei persoane fizice (numele societății este Vasile Ion SRL cu sediul la domiciliul domnului Vasile Ion, număr de telefon: numărul de telefon al domnului Vasile Ion).



Atenție! Normele se aplică, de asemenea, tuturor datelor cu caracter personal referitoare la persoane fizice în cadrul unei activități profesionale, cum ar fi angajații unei societăți, precum adresele de e-mail de afaceri ca prenume.num@societate.ro sau numerele de telefon ale angajaților.

În cazul în care este necesar a fi prelucrate date cu caracter personal, acestea ar trebui să fie **adecvate, relevante și limitate la ceea ce este necesar în scopul respectiv („reducerea la minimum a datelor”)**. În calitate de operator, societatea trebuie să evalueze ce volum de date este necesar și de a se asigura că nu se colectează date irelevante.



Exemplu: În cazul unei societăți care oferă persoanelor fizice servicii de închiriere a autoturismelor, se vor colecta și prelucra următoarele date: nume, adresa și numărul cardului de debit/credit al clienților și, poate, informații privind o eventuală dizabilitate de care suferă persoana în cauză (așadar, date privind sănătatea), dar nu și de originea rasială/sexul clienților.

Cui i se aplică GDPR? Este important unde are sediul o societate pentru a vedea dacă se aplică GDPR?

GDPR se aplică în cazul:

- unei societăți care prelucrează date cu caracter personal la sediul sau la sediul unei sucursale din UE sau
- unei societăți care are sediul în afara UE și oferă bunuri/servicii (contra cost sau gratuit) unor cetățeni ai unor țări membre UE sau monitorizează comportamentul unor persoane fizice din UE.

Exemplu când se aplică GDPR: O societate de recrutare cu activitate online și sediu în afara UE. Aceasta vizează în principal studenții din UE. Ea oferă consultanță gratuită cu privire la mai multe slujbe din SUA, iar studenții au nevoie de un nume de utilizator și o parolă pentru a accesa materialele online.

Exemplu când nu se aplică GDPR: O societate care este un portal de vânzare și închiriere de bunuri imobile dintr-o țară din afara UE. Societatea are sediul în afara UE și oferă servicii unor persoane din afara UE. Clienții pot utiliza aceste servicii când călătoresc în alte țări, inclusiv pe teritoriul UE. Atât timp cât serviciile prestate de societate nu se adresează în mod specific persoanelor fizice din UE, societatea nu face obiectul normelor GDPR.

Nu este relevantă dimensiunea companiei – GDPR-ul se aplică și societăților mari și societăților mici sau mijlocii (IMM) care prelucrează date conform descrierii de mai sus. Activitățile care prezintă riscuri ridicate pentru drepturile și libertățile persoanelor fizice, indiferent dacă sunt desfășurate de către un IMM sau de către o corporație, atrag aplicarea unor norme suplimentare, mai dure. Cu toate acestea, unele obligații prevăzute de GDPR nu li se aplică tuturor IMM-urilor.

De exemplu, societățile cu mai puțin de 250 de angajați nu au obligația să păstreze evidențe ale activităților lor de prelucrare decât dacă prelucrarea datelor cu caracter personal este o activitate regulată, reprezintă o amenințare la adresa drepturilor și a libertăților persoanelor fizice sau se referă la date sensibile ori la caziere judiciare.

Tot astfel, IMM-urile au obligația de a numi un responsabil cu protecția datelor numai dacă prelucrarea reprezintă activitatea lor principală și dacă aceasta implică anumite amenințări la adresa drepturilor și a libertăților persoanelor fizice (cum ar fi monitorizarea persoanelor fizice sau prelucrarea unor date sensibile ori a unor caziere judiciare), în special pentru că se desfășoară la scară largă.

Pentru a fi la curent cu prevederile legale în materie de protecție a datelor cu caracter personal, recomandăm operatorilor de date

consultarea permanentă a paginii web a Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal pe următoarea adresă: <http://www.dataprotection.ro/>. La secțiunea de legislație se pot observa trei subcapitole și anume Legislație internă, Legislație UE și Decizii A.N.S.P.D.C.P.

Norme GDPR obligatorii pentru toate societățile

GDPR a stabilit o serie de principii pe care toți operatorii de date cu caracter personal ar trebui să le urmeze, textul de lege fiind scris la nivel de recomandare, urmând ca DPO-ul să ajute la interpretarea adecvată a fiecărui principiu în scopul de a se asigura de respectarea acestora în acord cu obiectul de activitate al operatorului.

Aceste principii ghidează raționamentul DPO-ului în găsirea de soluții operaționale care să ajute la buna desfășurare a prelucrării, cu respectarea drepturilor persoanelor vizate. Cu alte cuvinte, principiile sunt liniile generale de avut în vedere la începutul oricărui tip de prelucrare.

Tipul și cantitatea de date cu caracter personal pe care societatea are dreptul să le prelucreze depind de motivul pentru care sunt prelucrate (temeiul juridic în cauză) și de scopul în care sunt prelucrate. Societatea/organizația trebuie să respecte mai multe norme-cheie, inclusiv următoarele:

- datele cu caracter personal trebuie prelucrate într-un mod legal și transparent, garantând echitatea în ceea ce privește persoanele fizice ale căror date cu caracter personal sunt prelucrate („legalitate, echitate și transparență”);
- trebuie să existe scopuri specifice ale prelucrării datelor și societatea trebuie să informeze persoanele fizice în legătură cu scopurile respective atunci când le colectează date cu caracter personal. Societatea nu poate colecta pur și simplu date cu caracter personal în scopuri nedefinite;
- societatea trebuie să colecteze și să prelucreze numai acele date cu caracter personal care sunt necesare pentru îndeplinirea scopului respectiv („reducerea la minimum a datelor”);
- societatea trebuie să se asigure că datele cu caracter personal sunt exacte și actualizate, având în vedere scopurile pentru care sunt prelucrate, și să fie corectate în caz contrar („exactitate”);
- societatea nu are dreptul să utilizeze datele cu caracter personal în alte scopuri care nu sunt compatibile cu scopul inițial;
- societatea trebuie să se asigure că datele cu caracter personal nu sunt stocate mai mult timp decât este necesar pentru scopurile în care au fost colectate („limitări legate de stocare”);

- societatea trebuie să prevadă garanții tehnice și organizaționale adecvate care să asigure securitatea datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnologice adecvate („integritate și confidențialitate”).



● **Exemplul 1:** Un magazin online trebuie să le explice clienților săi într-un limbaj clar și simplu politica sa de confidențialitate, de ce are nevoie de datele colectate, cum le va utiliza și cât timp intenționează să le păstreze.



● **Exemplul 2:** O societate care organizează un târg în cadrul căruia vizitatorii se înregistrează trebuie să comunice exact către cine și care dintre date vor ajunge la societățile care sunt expozante în cadrul respectivului târg.

Ce înseamnă „prelucrare a datelor”?

Prelucrarea datelor 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;

„Restricționarea prelucrării” înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora fie în vederea criptării sau anonimizării, fie atunci când o persoană ale cărei date au fost prelucrate a solicitat acest lucru, fie în vederea ștergerii acestora atunci când se împlinește termenul pe care societatea s-a angajat să îl respecte pentru păstrarea datelor.

Scopul prelucrării datelor. Pot fi prelucrate datele în orice scop?

Nu, scopul în care sunt prelucrate datele cu caracter personal trebuie cunoscut, iar persoanele fizice ale căror date sunt prelucrate trebuie informate. Nu se poate menționa pur și simplu că se vor colecta și prelucra date cu caracter personal. Acesta este principiul „limitărilor legate de scop”. Astfel, atât în mediul online (în cadrul politicii de confidențialitate cât și în