

CUPRINS

PARTEA I

Introducere în domeniul protecției datelor cu caracter personal / 11

CAPITOLUL 1

Noțiunile de bază referitoare la

Regulamentul General privind Protecția Datelor / 11

- 1.1. Istoricul domeniului protecției datelor cu caracter personal.
Analiza privind evoluția la nivel european și național a reglementărilor privind confidențialitatea datelor.
Ce aduce nou GDPR / 12
- 1.2. Cum impactează GDPR afacerile / 19
- 1.3. Cui se aplică GDPR / 25
- 1.4. Care sunt principiile unei prelucrări de date conforme și cum pot fi respectate acestea de către companii / 28
 - 1.4.1. Principiul echității, legalității și al transparenței / 28
 - 1.4.2. Principiul responsabilității / 32
 - 1.4.3. Principiul proporționalității și al necesității / 34
 - 1.4.4. Principiul reducerii la minim a datelor – minimizării datelor prelucrate / 35
 - 1.4.5. Principiul protecției implicite a datelor și al asigurării protecției datelor de la momentul conceperii / 36
- 1.5. Ce înseamnă „date cu caracter personal”, „date cu caracter special/sensibil”, „prelucrare de date”, „operator de date”, „persoana împuternicită cu prelucrarea datelor”
Noțiuni specifice GDPR / 38
- 1.6. Drepturile persoanei vizate în raport cu datele cu caracter personal / 49
 - 1.6.1. Dreptul de a fi informat / 50
 - 1.6.2. Dreptul de acces al unei persoane la datele proprii / 54
 - 1.6.3. Dreptul la rectificarea datelor / 56
 - 1.6.4. Dreptul la ștergerea datelor („dreptul de a fi uitat”) / 57
 - 1.6.5. Dreptul la restricționarea prelucrării / 58

| | | |
|--|---|----|
| 1.6.6. Dreptul la portabilitatea datelor | / | 59 |
| 1.6.7. Dreptul la opoziție | / | 60 |
| 1.7. Ce sunt incidentele de securitate a datelor, cum se previn și cum se raportează acestea către Autoritatea de Supraveghere | / | 62 |

CAPITOLUL 2

| | | |
|--|---|----|
| Responsabilul cu protecția datelor în companie (DPO) | / | 67 |
| 2.1. Cazuri obligatorii de desemnare a unui Responsabil cu Protecția Datelor (DPO) | / | 67 |
| 2.2. Cine poate fi DPO? | / | 72 |
| 2.3. Atribuții și îndatoriri ale DPO-ului | / | 75 |
| 2.4. Atribuțiile Responsabilului cu Protecția Datelor (DPO) | / | 78 |
| 2.5. Relația dintre DPO și conducerea societății | / | 80 |
| 2.6. Cum ne reprezintă DPO-ul compania? | / | 82 |

PARTEA 2

| | | |
|---|---|----|
| Implementarea practică a GDPR la nivelul IMM-urilor | / | 85 |
|---|---|----|

CAPITOLUL 3

| | | |
|---|---|-----|
| Politicile și procedurile de implementare GDPR în cadrul companiei | / | 85 |
| 3.1. Obligațiile companiilor pe linie de protecție a datelor | / | 85 |
| 3.2. Politicile și procedurile GDPR în cadrul companiei – cum le implementăm și care sunt persoanele responsabile de implementare | / | 89 |
| 3.2.1. Politici GDPR | / | 89 |
| 3.2.2. Proceduri GDPR | / | 93 |
| 3.3. Persoanele responsabile implicate în procesul de conformare a societății la normele GDPR | / | 98 |
| 3.4. Aplicarea GDPR în cadrul departamentelor societății. Provocări și elemente-cheie | / | 99 |
| 3.5. Obligații și situații practice privind relațiile de muncă | / | 100 |
| 3.5.1. Instruirea angajaților în domeniul protecției datelor – De ce? Când? Cum? | / | 100 |
| 3.5.2. Documentație GDPR specifică raporturilor de muncă | / | 102 |

| | | |
|--|---|-----|
| 3.5.2.1. Contractul Individual de Muncă – clauze specifice GDPR | / | 102 |
| 3.5.2.2. Nota de informare generală a angajaților | / | 105 |
| 3.6. Obligații și situații practice privind clienții | / | 115 |
| 3.6.1. Instrumente GDPR utile în relațiile comerciale | / | 117 |
| 3.7. Registrul de evidență a prelucrărilor de date | / | 120 |
| 3.8. Procedura în caz de incident de securitate a datelor | / | 125 |
| 3.8.1. Prevederi generale | / | 125 |
| 3.8.2. Procedura în caz de incident de securitate a datelor | / | 127 |
| 3.8.3. Cum se gestionează incidentul/ breșa de securitate? | / | 129 |
| 3.8.4. Ce sancțiuni se pot aplica pentru încălcarea procedurii cu privire la incidentele/ breșele de securitate? | / | 130 |
| 3.8.5. Cum se poate realiza informarea cu privire la încălcarea securității datelor cu caracter personal? | / | 131 |
| 3.8.6. Registrul incidentelor de securitate | / | 133 |
| 3.9. Procedura de exercitare a drepturilor persoanelor vizate | / | 134 |
| 3.9.1. Registrul cererilor persoanelor vizate | / | 147 |
| 3.10. Politica de retenție a datelor | / | 148 |

CAPITOLUL 4

Etapele implementării GDPR / 154

| | | |
|---|---|-----|
| 4.1. Auditul preliminar – instrument util de determinare a conformității unei companii | / | 155 |
| 4.1.1. Există un moment determinat în care auditul GDPR trebuie efectuat? | / | 156 |
| 4.1.2. Cine trebuie să efectueze auditul GDPR? Ce persoane din companie sunt implicate în această acțiune? | / | 157 |
| 4.1.3. Efectuarea auditului GDPR. Chestionarul de evaluare preliminară a proceselor de prelucrare | / | 158 |
| 4.2. Raportul de audit și Planul de conformare | / | 167 |
| 4.3. Implementarea prevederilor GDPR – activități și domenii vizate, departamente implicate, documentație specifică | / | 172 |
| 4.3.1. Accesul în sediul sau punctul de lucru al societății | / | 173 |

| | | |
|--|---|-----|
| 4.3.2. Prelucrarea datelor salariațiilor și candidațiilor – bune practici în cadrul departamentului de resurse umane (HR) | / | 175 |
| 4.3.3. Prelucrarea de date aparținând clienților | / | 178 |
| 4.3.4. Furnizorii și partenerii comerciali – tratarea proceselor de prelucrare desfășurate cu participarea persoanei împuternicite sau a operatorilor asociați | / | 179 |
| 4.3.5. Evidențe interne privind prelucrările de date, incidentele de securitate, precum și solicitările persoanelor vizate | / | 185 |
| 4.3.6. Proceduri și politici interne | / | 188 |
| 4.4. Măsurile tehnice și organizatorice de protecție a datelor personale | / | 189 |
| 4.4.1. Măsurile de ordin tehnic | / | 193 |
| 4.4.2. Măsurile de ordin organizatoric | / | 195 |
| 4.5. Privacy by design și privacy by default | / | 196 |
| 4.5.1. Confidențialitate prin proiectare / Data privacy by design | / | 197 |
| 4.5.2. Confidențialitate implicită/ Data by default | / | 198 |
| 4.6. Responsabilizarea angajaților și colaboratorilor pe linie de protecție a datelor | / | 200 |
| 4.6.1. Elaborarea de note de informare GDPR și aducerea la cunoștința salariațiilor a proceselor de prelucrare derulate, în primul rând, de angajator | / | 200 |
| 4.6.2. Includerea unor clauze privind protecția datelor cu caracter personal în Regulamentul Intern al societății | / | 201 |
| 4.6.3. Elaborarea fișelor de post în funcție de accesul la date pe care îl dețin angajații | / | 204 |
| 4.6.4. Încheierea de acorduri privind confidențialitatea datelor cu angajații | / | 206 |
| 4.6.5. Instruirea angajaților în materia protecției datelor | / | 206 |
| 4.7. Video-monitorizarea angajaților la locul de muncă – practică abuzivă sau necesară? | / | 207 |
| 4.7.1. Video-monitorizarea angajaților la locul de muncă potrivit Legii nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a GDPR | / | 211 |

CAPITOLUL 5

Conformarea site-urilor web la normele GDPR / 213

- 5.1. Categoriile de date prelucrate prin intermediul platformelor online / 215
 - 5.1.1. Formulare / 215
 - 5.1.2. Chatbot / 218
 - 5.1.3. Abonarea la newsletter / 220
 - 5.1.4. Cookie-uri / 220
 - 5.1.5. Recenzii (review-uri) / 222
 - 5.1.6. Wishlist-uri publice (liste de dorințe) / 222
 - 5.1.7. Harta ilustrând sediul societății / 223
 - 5.1.8. Videoclipurile de pe YouTube încărcate la nivelul website-urilor / 223
- 5.2. Persoanele vizate de prelucrările de date realizate prin intermediul platformelor online / 224
- 5.3. Documente GDPR obligatoriu de afișat pe website / 229
 - 5.3.1. Politica de confidențialitate / 229
 - 5.3.2. Politica de cookie-uri / 242
 - 5.3.3. Cookies pop-up/ widget/ banner/ icon / 248
 - 5.3.4. Politica de abonare la newsletter / 250
 - 5.3.5. Politica de call center / 253
 - 5.3.6. Texte tip GDPR disclaimers / 254
 - 5.3.7. Checklist documentație GDPR / 255
- 5.4. E-mail marketing – cum ne promovăm în mod legal business-ul prin newsletter. Condițiile unui consimțământ valabil acordat pentru primirea de mesaje comerciale și de marketing / 256
- 5.5. Procedura anti-SPAM / 263
- 5.6. Prelucrarea de date prin intermediul rețelelor de socializare / 265
- 5.7. Riscuri ale neconformării platformelor web la dispozițiile legale în materia protecției datelor / 269

PARTEA 3

Controalele pe tema GDPR / 273

CAPITOLUL 6

Sanționarea pentru nerespectarea GDPR / 273

6.1. Care este autoritatea competentă
ce sancționează operatorii de date / 273

6.2. Ce atribuții deține ANSPDCP / 276

6.3. Cum se poate depune o plângere la
Autoritatea de Supraveghere / 281

6.4. Procedura investigațiilor / 284

6.4.1. Controlul efectuat de ANSPDCP este întotdeauna anunțat? / 287

6.4.2. Se poate amâna efectuarea unei investigații anunțate? / 288

6.4.3. Desfășurarea efectivă a procedurii investigației / 289

6.4.3.1. Efectuarea investigațiilor pe teren / 290

6.4.3.2. Efectuarea investigațiilor la sediul ANSPDCP / 292

6.4.3.3. Efectuarea investigațiilor în scris / 293

6.4.4. Obligații ale entității controlate de ANSPDCP / 296

6.4.5. Procesul-verbal încheiat de ANSPDCP. Elemente componente / 296

6.5. Documente analizate de ANSPDCP în cazul unui control / 299

6.6. Ce sancțiuni și/sau măsuri corective poate impune ANSPDCP
unui operator de date și pe ce criterii se aplică acestea / 302

6.6.1. Individualizarea sancțiunilor / 305

6.6.2. Recomandări din partea ANSPDCP / 310

6.7. Exemple de sancțiuni și motive de aplicare a acestora / 311

6.8. Căi de atac ale procesului-verbal de sancționare de către ANSPDCP.
Litigii în materia protecției datelor supuse
instanțelor de judecată / 322

6.8.1. Dreptul de a formula Obiecțiuni / 322

Concluzii / 325

Note informative / 327