10 RECOMANDĂRI ESENȚIALE

pentru conformarea la GDPR

1. Drepturile persoanelor vizate

- ✓ Trebuie să **criptaţi datele prelucrate**. Acest lucru este esenţial atunci când vine vorba de protecţia datelor. Potrivit Comisiei Europene, dacă procesaţi date, trebuie să respectaţi reguli speciale pentru a asigura confidenţialitatea datelor clienţilor dvs., cum ar fi: pseudonimizarea, criptarea, confidenţialitatea etc.
- ✓ Trebuie să vă asiguraţi că clienţii dvs. îşi pot **retrage consimţământul** pentru utilizarea şi prelucrarea datelor. Potrivit comisiei UE, ar trebui să fie la fel de uşor să retrageţi consimţământul precum l-aţi acordat.

2. Consimțământul cu privire la colectarea și prelucrarea datelor

- ✓ Trebuie să implementaţi în compania dvs. **principiul minimizării datelor**, ceea ce înseamnă că trebuie să colectaţi doar datele care sunt absolut necesare despre fiecare client conform legislaţiei.
- ✓ Trebuie să obţineţi **permisiunea expresă a clientului** dvs. de a colecta şi de a folosi datele. Când este vorba de acordul persoanei vizate, Comisia UE este foarte strictă.
- ✓ Nu colectaţi mai multe date decât este necesar. De multe ori, datele furnizate de persoanele fizice sunt folosite cu scop diferit faţă de cel propus si uneori, nu sunt folosite deloc. O astfel de procedură stufoasă, poate să atragă după sine răspundere contravenţională.

3. Protecția datelor prin aplicarea principiului "Privacy by design"

- ✓ **Privacy by design** înseamnă dezvoltarea de proiecte noi având ca punct de focus protecția datelor cu caracter personal. Fie că ne referim la proiecte informatice, legi, regulamente sau politici noi, trebuie să avem în vedere protejarea intereselor persoanei vizate.
- ✓ Urmând acest concept, puteți identifica încă de la început punctele slabe și posibilele probleme, ușurându-vă astfel considerabil munca.

4. Gestionarea breșelor de securitate

- ✓ Trebuie să implementați un **plan de notificare privind încălcarea datelor**. În cazul unei încălcări a datelor, dacă sunteți operator de date, aveți **72 de ore** la dispoziție să notificați autoritatea de supraveghere. Va trebui să comunicați informații specifice, cum ar fi natura încălcării datelor cu caracter personal, numele persoanelor vizate, consecințele acestei încălcări a datelor și acțiunile dvs. de remediere a acesteia.
- ✓ Vă recomandăm **GDPR Audit**, un soft special dezvoltat pentru astfel de nevoi care ține evidența prelucrărilor, criptează, securizează si alertează potențialele scurgeri de date.

5. Verificarea datelor, inventarierea și evidențierea tipurilor de prelucrări

- ✓ Trebuie să stabiliți **o hartă clară a datelor înregistrate**. Acest inventar de date trebuie să includă informații precum scopul prelucrării, descrierea tipului de date înregistrate, persoana responsabilă, baza legală pentru stocarea datelor și persoanele care au acces la aceste date. Aceasta trebuie să fie actualizată periodic.

6. Furnizori și colaboratori terți implicați în colectarea și prelucrarea datelor

- ✓ În contextul Regulamentului, noțiunea de **terț** se definește ca o persoană fizică sau juridică, autoritate publică, agenție sau un organism, alta decât persoana vizată sau procesatorul, aflată sub directa autoritate a operatorului sau a procesatorului, autorizate să proceseze date cu caracter personal.
- ✓ Datorită utilizării pe scară largă a serviciilor externalizate, una dintre cele mai exigente sarcini în pregătirea GDPR este evaluarea riscurilor din partea terților. **Operatorii de date sunt responsabili pentru acțiunile întreprinse de procesatorii lor**, deci este important să identificați toți procesatorii relevanți, să înțelegeți ce date sunt stocate și procesate de aceștia, cât de bine protejează fiecare procesator datele și progresele înregistrate de aceștia pentru a deveni conformi cu GDPR.
- ✓ Pentru a vă asigura că vă aflați în acest punct, puteți urma cei 10 pași din articolul: Cum ne pregătim pentru GDPR în 10 pași

7. Politica de confidențialitate

- ✓ Trebuie să **actualizați documentația** disponibilă pentru public, cum ar fi politica de confidențialitate și modalitățile de obținere a acordului. În plus, asigurați-vă că informațiile dvs. respectă regulile privind politicile GDPR (informațiile trebuie să fie concise, transparente, inteligibile, ușor accesibile etc.).

8. Conștientizarea personalului și a conducerii

- ✓ Trebuie să **informați echipa** despre protecția datelor clienților dvs.! Drumul spre respectarea GDPR nu este ușor și nu implică faptul că doar o persoană din companie este în cunoștință, ci este un efort unitar. Toți cei din companie ar trebui să contribuie la confidențialitatea datelor, de aceea,

prin instruire, cursuri sau prezentări vă veți ajuta să satisfaceți împreună cerințele.

9. Responsabilul cu protecția datelor - DPO

- ✓ Toate instituțiile publice precum și majoritatea companiilor private vor avea obligativitatea de a numi un DPO începând cu data de 25 mai 2018.
- ✓ Ofițerul responsabil pentru protecția datelor cu caracter personal sau DPO-ul, poate fi un angajat din cadrul organigramei sau poate fi contractat extern.
- ✓ Înainte de a lua o hotărâre privitoare la DPO trebuie să fiți atenți la specificațiile acestui post. În primul rând responsabilul cu protecția datelor trebuie să fie independent. Acesta nu poate fi sancționat nici concediat pentru îndeplinirea atribuțiilor sale. Este necesar să aibă acces la toate operațiunile de prelucrare a datelor până la cel mai înalt nivel al conducerii.

10. Informarea corectă

Sunt multe informații legate de Regulament și este greu să le parcurgeți pe toate pentru ca mai apoi să selectați ce este important.

Cea mai buna metodă de a ști ce înseamnă GDPR și mai ales cum vă afectează, este să citiți, ca și punct de plecare, chiar textul Regulamentului GDPR.