

POLITICII DE PROTECȚIE A DATELOR

1. Obiectiv

Scopul politicii de protecție a datelor este reprezentarea aspectelor legale privind protecția datelor într-un singur document de sinteză. De asemenea, poate fi folosit ca bază pentru inspecțiile legale privind protecția datelor, de ex. de către client în domeniul prelucrării comandate. Acest lucru nu este numai pentru a asigura respectarea Regulamentului european general privind protecția datelor (GDPR), ci și pentru a furniza dovada conformității.

2. Preambul

Scurtă descriere a companiei și motivația de a respecta protecția datelor.

3. Politica de securitate și responsabilitățile companiei

- Pentru o companie, pe lângă obiectivele corporative existente, trebuie definite și documentate cele mai înalte obiective de protecție a datelor. Obiectivele privind protecția datelor se bazează pe principiile de protecție a datelor și trebuie modificate individual pentru fiecare companie.
- Determinarea rolurilor și responsabilităților (de exemplu, reprezentanți ai companiei, ofițeri operaționali de protecție a datelor, coordonatori sau echipa de protecție a datelor și manageri operaționali)
- Angajamentul de îmbunătățire continuă a unui sistem de management al protecției datelor
- Instruirea, sensibilizarea și obligația angajaților

4. Cadrul legal în cadrul companiei

- Reguli legale sau de conduită specifice industriei pentru tratarea datelor cu caracter personal
- Cerințele părților interne și externe
- Legile aplicabile, eventual cu reglementări locale speciale

5. Documentație

- A efectuat inspecții interne și externe
- Necesitatea protecției datelor: determinarea necesității de protecție cu privire la confidențialitate, integritate și disponibilitate.

6. Măsurile tehnice și organizatorice existente

Măsuri tehnice și organizatorice adecvate care trebuie puse în aplicare și justificate, luând în considerare, printre altele, scopul prelucrării, stadiul tehnologiei și costurile de punere în aplicare.

Descrierea măsurilor tehnice și organizatorice implementată poate fi bazată, de exemplu, pe structura ISO / IEC 27002, ținând seama de ISO / IEC 29151 (orientări pentru protecția datelor cu caracter personal). Capitolele respective trebuie să fie justificate prin referirea la liniile directoare existente.

Exemple de astfel de orientări includ:

- Orientări privind drepturile persoanelor vizate
- Controlul accesului
- Clasificarea informațiilor (și manipularea acestora)
- Securitatea fizică și de mediu pentru utilizatorii finali, cum ar fi:
 - Utilizarea permisă a valorilor
 - Ghid pentru transferul de informații în funcție de mediul de lucru și blocările ecranului
 - Dispozitive mobile și telecomunicații
 - Restricționarea instalării și utilizării software-ului
- Copia de rezerva a datelor
- Transfer de informații
- Protecția împotriva programelor malware
- Manipularea punctelor slabe tehnice
- Măsuri criptografice
- Securitatea comunicării
- Confidențialitatea și protecția informațiilor personale
- Relațiile furnizorilor: Notă inspecția și evaluarea periodică a procesării datelor, în special eficacitatea măsurilor tehnice și organizatorice implementate.