



TRUSTED.RO

Marca de Încredere
din comerțul electronic românesc

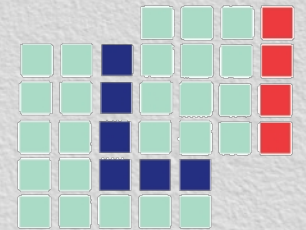
Implementarea GDPR: două probleme majore

și câteva soluții pentru un client
tip magazin online

Bogdan Manolea
Co-Fondator TRUSTED.ro

Cine este TRUSTED.ro, cine sunt eu

- De peste 7 ani, acordăm Marca de Încredere TRUSTED.ro, pe baza unui set de criterii legale și de bune practici.
- De peste 20 de ani, scriu (*și învăț*) despre drept și tehnologie. Uneori și predau.



legi-internet.ro



TRUSTED.RO

Problema nr. 1 – Ștergerea datelor

- Art 5 (1) e)
- păstrate într-o formă care permite identificarea persoanelor vizate **pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor** în care sunt prelucrate datele (principiul “stocării limitate”)

Problema nr. 1 – Ștergerea datelor

- Adică:
- Toate datele personale trebuie șterse* la un moment dat.

* Există și posibilitatea de a le transforma în date anonime.

Când le ștergem?!?

Și întrebarea “cum le ștergem?” este importantă,
dar dincolo de scopul prezentării

Problema nr. 1 – Ștergerea datelor

- Răspuns corect: Depinde.
- Indiciu – art. 13 (2) a) Informarea persoanelor *perioada pentru care vor fi stocate datele cu caracter personal sau dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă*

Soluția nr. 1 – Ștergerea datelor

- Pentru un magazin online, ne putem gândi la diverse tipuri de date și scopuri:
 1. Datele necesare încheierii contractului (Temei legal) Art 6 (1) (b)
Perioada posibilă:
 - Perioada desfășurării contractului, *sau*
 - Perioada desfășurării contractului + 3 ani (termenul de prescripție generală)

Soluția nr. 1 – Ștergerea datelor

2. Datele necesare îndeplinirii unei obligații legale (Temei legal - Art 6 (1) (c))

Perioada cf OMFP nr. 2634/2015:

- State de plată salarii – 50 de ani
- Registre contabilitate – 10 ani
- Chitanțe – 5 ani

Soluția nr. 1 – Ștergerea datelor

3. Datele pentru marketing – ex. newsletter (Temei legal - Art 6 (1) (a) - consimțământ)

Perioada posibilă:

- Până la retragerea consimțământului?
- 30 de zile de la ultima interacțiune?
- Soft-bounce sau hard-bounce?
- Altele ? (cutume, bune practici ale industriei)

Problema 2 – Încălcarea securității

- Art 33 GDPR
- În cazul în care are loc o **încălcare a securității datelor cu caracter personal**, operatorul notifică acest lucru (...), fără întârzieri nejustificate și, dacă este posibil, **în termen de cel mult 72 de ore** de la data la care a luat cunoștință de aceasta (...)

Problema 2 – Încălcarea securității

- „încălcarea securității datelor cu caracter personal” înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la **distrugerea, pierderea**, modificarea, sau divulgare a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau **la accesul neautorizat la acestea**.

Problema 2 – Încălcarea securității

- Principiu – Notificarea autorității în 72 de ore
- Dar poate și către persoanele vizate, dacă “este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice”
- Detalii în Opinia Grupului de Lucru Art. 29 – WP250rev.01 (6.02.2018)

Soluții 2 – Încălcarea securității

- Identificarea încălcărilor de securitate
- Identificarea riscului pentru persoanele vizate
- Notificări legale (Autoritate și persoane vizate)
- Documentarea și înregistrarea încălcării securității

Soluții 2 – Încălcarea securității

Adoptarea măsurilor de securitate care nu necesită notificarea (nu există risc pentru persoane), cum ar fi:

- Colectarea de date deja disponibile public
- Date criptate (bine)
- Date neinteligibile pentru terțe părți (pseudonimizare?)

Dar, în orice caz, trebuie documentate.

- Dispoziții contractuale precise cu împuterniciții (inclusiv posibilitatea de a face notificarea în locul operatorului)





TRUSTED.RO

Marca de Încredere
din comerțul electronic românesc

Q&A

Muțumesc!

[TRUSTED.ro](https://www.trusted.ro)

contact@trusted.ro