Site compromis.

Este automat și o breșă GDPR?

Cum investigăm, documentăm și decidem dacă trebuie notificată ANSPDCP

Un ghid practic pentru DPO, manageri și echipe IT, realizat de

GDPR COMPLET®

Scenariul clasic

> „Am identificat scriptul, l-am șters, am schimbat parolele și am instalat măsuri suplimentare de securitate."

Foarte bine. Din perspectiva IT, incidentul este remediat. Dar din perspectiva GDPR, remedierea tehnică deschide, nu închide, investigația.

Întrebarea esențială: Ce s-a întâmplat *înainte* să îl ștergem? Cât timp a fost activ? Ce a putut accesa? Ce date au fost expuse?

Remedierea IT

Script șters, parole schimbate, vulnerabilitate remediată. Incidentul tehnic este închis.

Investigația GDPR

Abia acum începe evaluarea: ce date au fost expuse, cui și cu ce risc.

Decizia de notificare

Pe baza investigației se decide dacă există obligații față de ANSPDCP și față de persoanele vizate.

Trei etape diferite — nu una singură

Cel mai frecvent confuzie: tratarea remedierii tehnice ca și cum ar fi și concluzia GDPR. Sunt trei procese distincte, cu obiective diferite.

1. Containment / Remediere

- Site offline sau izolat
- Script malițios șters
- Parole schimbate
- Vulnerabilitate remediată

2. Investigație

- Cum a intrat atacatorul?
- De când era activ codul?
- Ce acces a obținut?
- Ce a modificat sau exfiltrat?

3. Evaluare GDPR

- Au fost afectate date personale?
- Ce risc există pentru persoanele vizate?
- Notificăm ANSPDCP? (art. 33)
- Informăm persoanele vizate? (art. 34)

Principiu fundamental: Remedierea tehnică nu înlocuiește evaluarea incidentului din perspectiva protecției datelor personale.

GDPR COMPLET®

Incident IT ≠ automat Personal Data Breach

Distincția conceptuală este esențială pentru a evita atât sub-raportarea, cât și supra-raportarea incidentelor.

Personal Data Breach — definiție

Presupune: acces neautorizat, divulgare, pierdere, modificare, distrugere sau indisponibilitate relevantă a datelor cu caracter personal prelucrate de operator.

Incident de securitate IT

Un site compromis este, prin definiție, un incident de securitate IT. Acesta poate sau nu să implice date personale.

Condiția de transformare

Incidentul IT devine personal data breach **numai dacă** a afectat date personale prelucrate de operator — prin acces, modificare, exfiltrare sau indisponibilitate.

Concluzie operațională

Site compromis = incident de securitate.
Site compromis ≠ automat breșă GDPR.
Investigația stabilește dacă și în ce măsură datele personale au fost afectate.

De ce contează distincția?

Notificarea prematură sau nejustificată poate crea obligații inutile și poate distrage atenția de la investigația reală. Lipsa notificării atunci când este necesară atrage răspundere. Investigația corectă este singura cale.

GDPR COMPLET®

Două direcții ale investigației

Același incident poate genera efecte în două direcții complet diferite, care necesită investigații paralele și independente.

A. Infrastructura companiei

„Ce a putut vedea atacatorul?"

- Acces la panoul WordPress admin
- Acces la baza de date (utilizatori, comenzi, formulare)
- Formulare de contact, abonamente, conturi
- Loguri de autentificare și sesiuni active
- Fișiere de configurare cu credențiale

B. Vizitatorii site-ului

„Ce a primit utilizatorul?"

- Script injectat executat în browserul vizitatorului
- Redirecționare malițioasă către site terț
- Fake CAPTCHA sau verificare falsă
- Descărcare de malware pe dispozitivul utilizatorului
- Colectare potențială de date introduse în formulare

Același incident, două evaluări distincte: Impactul asupra infrastructurii operatorului și impactul asupra vizitatorilor trebuie analizate separat. Concluzia poate fi diferită pentru fiecare direcție.

Exemplu real, anonimizat: un site legitim transformat în vector de atac

Cazul ilustrează cum un incident tehnic aparent limitat poate implica efecte complexe asupra vizitatorilor, fără ca datele operatorului să fie neapărat compromise.

1

Compromitere inițială

Site legitim compromis prin injectare de cod malițios în fișierele front-end.

2

Inginerie socială

Vizitatorii prezentați cu o falsă verificare Cloudflare, aparent legitimă.

3

Execuție malware

Utilizatorul determinat să execute o comandă PowerShell pe propriul dispozitiv.

4

Payload suplimentar

Componentă malware descărcată; blocată de antivirus în cazul documentat.

Ce știm

Mecanismul de atac era funcțional. Vizitatorii au fost expuși unui vector de inginerie socială. Codul era activ pe site.

Ce nu știm automat

Nu știm dacă datele operatorului (baza de date, formulare, conturi) au fost compromise. Aceasta este tocmai întrebarea investigației GDPR — nu o concluzie implicită.

Întrebarea nr. 1: Ce acces a obținut atacatorul?

Nivelul de acces obținut de atacator definește ce date puteau fi accesate sau exfiltrate. Aceasta este variabila centrală a evaluării GDPR.

1	**Nivel 1 — Modificare limitată** Modificare a unui script sau fișier front-end. Acces minim, fără privilegii administrative. Risc redus pentru datele operatorului.
2	**Nivel 2 — Acces WordPress Admin** Acces la panoul de administrare. Poate vizualiza utilizatori, conținut, setări, unele date din formulare.
3	**Nivel 3 — Acces FTP/SFTP/Hosting** Acces la fișierele serverului, inclusiv fișiere de configurare cu credențiale de bază de date.
4	**Nivel 4 — Acces bază de date / server** Acces direct la toate datele stocate: utilizatori, comenzi, formulare, date personale. Risc ridicat.
5	**Nivel 5 — Exfiltrare confirmată** Dovezi că datele au fost copiate sau transmise în afara sistemului. Cel mai grav scenariu. Notificare aproape certă.

Relevanță pentru DPO: Vulnerabilitatea tehnică nu este doar o problemă IT — ea definește perimetrul datelor care puteau fi accesate și, implicit, obligațiile GDPR.

T0 și T1 — Cât timp a fost activ incidentul?

Perioada de expunere este o variabilă critică: determină câți vizitatori au fost potențial afectați și ce date au putut fi accesate în intervalul respectiv.

T0 — Prima compromitere

1

Prima apariție a codului malițios, identificată din backup-uri, loguri sau timestamp-uri ale fișierelor modificate.

2

Perioadă de expunere

Intervalul în care codul malițios era activ și vizitatorii puteau fi afectați. Aceasta este fereastra de risc.

T1 — Remediere

3

Momentul în care site-ul a fost oprit sau codul a fost eliminat. Incidentul tehnic este închis.

Surse pentru reconstituire

- WAF / CDN logs (Cloudflare, Sucuri etc.)
- Audit logs WordPress
- FTP / SSH / SFTP access logs
- Backup-uri anterioare incidentului
- Timestamp-uri ale fișierelor modificate

De ce contează perioada?

Fără T0 nu putem estima numărul vizitatorilor expuși. Fără T1 nu putem confirma că incidentul s-a încheiat. Fără ambele, evaluarea riscului rămâne incompletă și documentarea GDPR este vulnerabilă.

Nu putem evalua impactul fără a cunoaște perioada de expunere.

GDPR COMPLET®

Câți vizitatori au fost expuși?

Numărul de vizitatori ai site-ului în perioada de expunere nu este automat numărul persoanelor afectate. Scripturile malițioase sunt adesea selective în livrare.

Filtrare după browser

Unele scripturi se activează doar în anumite browsere sau versiuni specifice, excluzând automat o parte din vizitatori.

Filtrare după IP / geoloc

Atacatorii pot limita livrarea payload-ului la anumite regiuni geografice sau adrese IP pentru a evita detectarea.

Filtrare după sursă de trafic

Scriptul poate fi activ doar pentru utilizatorii veniți din motoare de căutare, nu pentru accesul direct sau din rețele sociale.

Filtrare după pagini

Codul malițios poate fi injectat doar în anumite pagini, nu pe întregul site, limitând expunerea la vizitatorii acelor pagini.

Concluzie metodologică: Analiza logurilor și a comportamentului scriptului este esențială pentru a delimita expunerea reală. Numărul total de vizitatori este un plafon maxim, nu o cifră exactă a persoanelor afectate.

Trebuie notificată automat ANSPDCP?

NU.

Mai întâi stabilim dacă avem un personal data breach și evaluăm riscul. Notificarea este o consecință a evaluării, nu un reflex automat.

Fluxul decizional corect

01

Incident IT identificat

Au fost afectate date personale? Dacă **NU** → documentare și închidere.

02

Date personale compromise

Evaluare risc pentru persoanele vizate. Dacă riscul este **probabil** → art. 33 GDPR → notificare ANSPDCP în 72h.

03

Risc ridicat identificat

Evaluare suplimentară art. 34 GDPR → informarea directă a persoanelor vizate, fără întârzieri nejustificate.

Incident IT fără date personale

Documentare internă. Nicio obligație de notificare ANSPDCP.

Breșă cu risc improbabil

Documentare obligatorie (registrul intern). Notificare ANSPDCP — analiză de la caz la caz.

Breșă cu risc probabil

Notificare ANSPDCP (art. 33). Dacă risc ridicat → informare persoane vizate (art. 34).

GDPR COMPLET®

Cele 72 de ore — când începe termenul?

Art. 33 GDPR prevede notificarea autorității de supraveghere **în termen de 72 de ore** de la momentul în care operatorul a luat cunoștință de breșă — nu de la momentul remedierii tehnice.

Momentul de start al termenului

Termenul curge din momentul în care operatorul are un **grad rezonabil de certitudine** că a avut loc o încălcare a securității datelor personale. Nu este necesar să fie finalizată investigația completă.

Investigația inițială este permisă

O perioadă scurtă de investigație pentru a confirma natura incidentului este acceptabilă. Aceasta **nu poate fi prelungită artificial** pentru a amâna notificarea.

Notificare parțială, completată ulterior

Dacă nu sunt disponibile toate informațiile în 72h, notificarea poate fi transmisă cu datele disponibile și **completată ulterior**, cu menționarea motivului întârzierii.

⚠ **Atenție:** Nu aștepta finalizarea unui forensic de două săptămâni dacă deja ai un grad rezonabil de certitudine că incidentul este notificabil. Termenul curge indiferent de stadiul investigației tehnice.

Nu șterge probele odată cu malware-ul

Una dintre cele mai frecvente erori: în graba de a remedia incidentul, echipa IT șterge sau suprascrie exact probele de care DPO va avea nevoie pentru documentare și evaluare.

Ce trebuie păstrat

- Access logs, error logs, WordPress logs
- WAF / CDN logs (Cloudflare, Sucuri etc.)
- Loguri de autentificare (admin, FTP, SSH, SFTP)
- Copie a scriptului malițios și a fișierelor compromise
- Backup anterior incidentului
- Lista pluginurilor active și versiunile lor
- Lista utilizatorilor administrativi la momentul incidentului
- Timestamp-uri relevante pentru cronologie

De ce este critic

Fără probe, poți remedia incidentul tehnic — dar ulterior nu mai poți demonstra ce s-a întâmplat, ce date au fost sau nu au fost accesate, și de ce decizia de notificare (sau de ne-notificare) a fost corectă.

Documentarea GDPR nu se poate construi retroactiv din memorie. Probele sunt baza oricărei evaluări credibile.

Procedură recomandată: Înainte de orice remediere, echipa IT arhivează toate logurile și o copie a fișierelor compromise. Abia apoi începe curățarea.

Cele 8 întrebări la care DPO trebuie să aibă răspuns

DPO nu trebuie să efectueze investigația forensic. Trebuie să știe ce să întrebe echipa IT și să evalueze răspunsurile din perspectiva protecției datelor.

1 **Unde a fost găsit codul malițios?**

Fișier front-end, plugin, temă, fișier de configurare, bază de date?

2 **Cum a fost introdus?**

Plugin vulnerabil, credențiale compromise, vulnerabilitate server, acces neautorizat la panou?

3 **De când era activ?**

T0 identificat din loguri, backup-uri sau timestamp-uri de fișiere?

4 **Ce privilegii a obținut atacatorul?**

Nivel 1–5 conform scalei de acces. Acces limitat sau acces complet la sistem?

5 **Putea accesa baza de date?**

Existau credențiale expuse? A existat acces direct la tabele cu date personale?

6 **Există indicii de exfiltrare?**

Trafic de ieșire neobișnuit, conexiuni externe, fișiere create sau transferate?

7 **Câte persoane au fost expuse?**

Număr estimat de vizitatori în perioada T0–T1, cu filtrele de livrare ale scriptului?

8 **Ce probe și loguri avem disponibile?**

Ce a fost arhivat înainte de remediere? Ce mai poate fi recuperat?

GDPR COMPLET®

Concluzia: trei rezultate posibile

Orice investigație a unui site compromis trebuie să conducă la una dintre cele trei concluzii de mai jos. Scopul nu este să demonstrăm că avem sau nu avem o breșă — ci să avem suficiente informații pentru a argumenta concluzia corectă.

A. Incident IT fără personal data breach

Investigația confirmă că datele personale nu au fost afectate. Acțiune: documentare internă și închidere. Nicio obligație de notificare ANSPDCP.

B. Personal data breach cu risc improbabil

Date personale afectate, dar riscul pentru persoanele vizate este improbabil. Acțiune: documentare obligatorie în registrul intern; analiză privind oportunitatea notificării.

C. Personal data breach cu risc probabil

Date personale afectate, risc probabil pentru persoanele vizate. Acțiune: evaluare și notificare ANSPDCP (art. 33). Dacă risc ridicat → evaluare art. 34 și informarea persoanelor vizate.

> Nu încercăm să demonstrăm că avem o breșă GDPR. Încercăm să avem suficiente informații pentru a demonstra de ce este sau de ce nu este o breșă GDPR.

Notă

Material informativ. Fiecare incident necesită evaluare individuală în funcție de circumstanțele specifice, tipul de date prelucrate și contextul organizației. Conținutul acestui material nu constituie consultanță juridică.