



GESTIONAREA INCIDENTELOR DE SECURITATE ȘI NOTIFICAREA BREȘELOR

Șablon ghidat, conform art. 33–34 GDPR · Ediția 2026

Un șablon în două părți: procedura internă de gestionare a incidentelor și modelele de notificare (către ANSPDCP și către persoanele vizate). Se folosește împreună cu Registrul breșelor de securitate (fișier Excel separat).

Material informativ oferit gratuit de STABRIS

Cum utilizați acest șablon

Acesta NU este o procedură gata de implementat, ci un cadru care vă arată etapele obligatorii și câmpurile notificărilor. Partea I descrie procedura internă, iar Partea a II-a conține modelele de notificare. În fiecare secțiune găsiți un Ghid și un câmp marcat cu .

Ceasul de 72 de ore: *din momentul în care luați cunoștință de o breșă, aveți cel mult 72 de ore pentru a notifica ANSPDCP (art. 33). Dacă breșa prezintă risc ridicat, trebuie informate și persoanele vizate (art. 34). Decizia dacă breșa este notificabilă — și dacă riscul este «ridicat» — se ia printr-o evaluare a riscului, de la caz la caz. O evaluare greșită (fie omisiunea notificării, fie supra-notificarea) are consecințe. Sub presiunea celor 72 de ore, sprijinul de specialitate este decisiv.*

De reținut: *șablonul vă arată etapele și câmpurile obligatorii. Evaluarea riscului (nucleul deciziei de notificare), playbook-urile de limitare a incidentului și fluxul de escaladare adaptat organizației dvs. reprezintă chiar obiectul serviciilor STABRIS — inclusiv al sprijinului de urgență în primele ore de la constatare.*

PARTEA I — PROCEDURA INTERNĂ DE GESTIONARE A INCIDENTELOR

(etapele de parcurs din momentul detectării unui incident)

I.1. Detectarea și raportarea internă

Ghid — ce trebuie să conțină: Orice angajat care observă un posibil incident îl raportează imediat unui punct unic de contact. Cu cât mai devreme este detectat, cu atât mai ușor se respectă termenele.

 [Completați: canalul de raportare internă și responsabilul]

I.2. Înregistrarea și clasificarea inițială

Ghid — ce trebuie să conțină: Înregistrați incidentul și stabiliți dacă este o breșă de date cu caracter personal și ce tip: de confidențialitate (divulgare/acces neautorizat), de integritate (alterare) sau de disponibilitate (pierdere/indisponibilitate).

 [Completați: modul de înregistrare și clasificare]

I.3. Limitarea incidentului (containment)

Ghid — ce trebuie să conțină: Măsuri imediate pentru a opri sau limita breșa și efectele ei (izolarea sistemelor, revocarea accesului, recuperarea datelor).

 [Completați: măsurile de limitare și cine le dispune]

I.4. Evaluarea riscului pentru drepturile și libertățile persoanelor

Ghid — ce trebuie să conțină: Etapa decisivă: stabiliți probabilitatea și gravitatea riscului pentru persoanele vizate. Rezultatul determină dacă breșa se notifică și dacă trebuie informate persoanele. Această evaluare se face de la caz la caz, după o metodologie de analiză a riscului.

 [A se realiza printr-o evaluare a riscului — element de specialitate]

I.5. Decizia privind notificarea ANSPDCP (72 de ore)

Ghid — ce trebuie să conțină: Breșa se notifică ANSPDCP fără întârzieri nejustificate și, dacă este posibil, în cel mult 72 de ore de la constatare, cu excepția cazului în care este puțin probabil să genereze un risc pentru persoane. Dacă notificarea întârzie, se justifică motivele — art. 33 alin. 1.

 [Completați: fluxul decizional și cine aprobă notificarea]

I.6. Comunicarea către persoanele vizate (risc ridicat)

Ghid — ce trebuie să conțină: Dacă breșa prezintă un risc ridicat, persoanele vizate se informează fără întârzieri nejustificate, în limbaj clar. Există excepții (ex. date criptate, măsuri ulterioare care elimină riscul) — art. 34.

 [Completați: criteriile și canalul de informare a persoanelor]

I.7. Documentarea în registrul breșelor

Ghid — ce trebuie să conțină: TOATE breșele se documentează (fapte, efecte, măsuri), indiferent dacă au fost sau nu notificate — obligație de sine stătătoare, art. 33 alin. 5. Vezi Registrul breșelor (fișier Excel).

 [A se completa în Registrul breșelor]

I.8. Măsuri corective și lecții învățate

Ghid — ce trebuie să conțină: După soluționare, analizați cauzele și luați măsuri pentru a preveni repetarea (actualizarea măsurilor de securitate, instruire).

 [Completați: procesul de analiză post-incident]

PARTEA A II-A — MODELE DE NOTIFICARE

II.A. Notificarea către ANSPDCP (art. 33 alin. 3)

Se transmite autorității prin canalul oficial de notificare a incidentelor. Conținutul minim obligatoriu:

II.A.1. Operatorul

Ghid — ce trebuie să conțină: Datele de identificare ale operatorului.

 [Completați: denumire și date de contact]

II.A.2. Persoana de contact / DPO

Ghid — ce trebuie să conțină: Numele și datele de contact ale DPO sau ale punctului de la care se pot obține mai multe informații — art. 33(3) (b).

 [Completați: date de contact DPO / punct de contact]

II.A.3. Natura breșei

Ghid — ce trebuie să conțină: Descrierea caracterului breșei (ce s-a întâmplat, tipul de breșă) — art. 33(3) (a).

 [Completați: descrierea naturii breșei]

II.A.4. Categoriile și numărul aproximativ de persoane vizate

Ghid — ce trebuie să conțină: Câte și ce categorii de persoane sunt afectate (estimare) — art. 33(3) (a).

 [Completați: categorii și număr aproximativ de persoane]

II.A.5. Categoriile și numărul aproximativ de înregistrări

Ghid — ce trebuie să conțină: Volumul aproximativ de înregistrări de date afectate — art. 33(3) (a).

 [Completați: categorii și număr aproximativ de înregistrări]

II.A.6. Consecințele probabile

Ghid — ce trebuie să conțină: Ce efecte poate avea breșa asupra persoanelor — art. 33(3) (c).

 [Completați: consecințele probabile]

II.A.7. Măsurile luate sau propuse

Ghid — ce trebuie să conțină: Măsurile de remediere și de atenuare a efectelor — art. 33(3) (d).

 [Completați: măsurile luate/propuse]

II.A.8. Cronologia și, dacă este cazul, motivele întârzierii

Ghid — ce trebuie să conțină: Momentul constatării și, dacă notificarea depășește 72 de ore, motivele întârzierii — art. 33(1).

 [Completați: cronologia și eventualele motive de întârziere]

II.B. Comunicarea către persoanele vizate (art. 34)

Ghid — ce trebuie să conțină: Se face numai când breșa prezintă risc ridicat. Trebuie să descrie, în limbaj clar, natura breșei, datele de contact ale DPO, consecințele probabile și măsurile luate/recomandate persoanelor. Verificați întotdeauna dacă se aplică vreuna dintre excepțiile de la art. 34 alin. 3.

 [Completați: mesajul către persoanele vizate, dacă riscul este ridicat]

Ce urmează?

STABRIS poate:

- construi procedura de gestionare a incidentelor și playbook-urile de limitare adaptate organizației dvs.;
- defini metodologia de evaluare a riscului care determină dacă breșa se notifică;
- oferi sprijin de urgență în primele ore de la constatarea unei breșe (redactarea și transmiterea notificărilor);
- prelua rolul de DPO extern și punct de contact pentru ANSPDCP.

Ați avut o breșă? Solicitați sprijin de urgență în cele 72 de ore.

Website: [www.stabris.ro] **Email:** [contact@stabris.ro] **Telefon:** [0332.402.192]

Disclaimer. Prezentul șablon este un material orientativ și informativ, oferit gratuit de STABRIS. Nu constituie consultanță juridică sau de specialitate și nu reprezintă o procedură gata de implementat. Decizia de notificare depinde de o evaluare a riscului, care se face de la caz la caz. © 2026 STABRIS. Toate drepturile rezervate.