**Incidentele de securitate a datelor potrivit GDPR. Cum le recunoaștem și calificăm corect?**

Situațiile în care operatorii de date cu caracter personal se pot confrunta cu incidente de securitate a datelor ce ridică riscuri pentru drepturile și libertățile persoanelor vizate sunt numeroase. În astfel de cazuri, operatorii de date sunt nevoiți, printre altele, să notifice respectivele incidente către autoritatea de supraveghere competentă și către persoanele vizate, după caz, în linie cu prevederile GDPR.

Uneori, pașii inițiali privind recunoașterea unui incident și corecta calificare a acestuia pot reprezenta o provocare pentru operatorii de date, având în vedere scenariile extrem de frecvente și variate în care acestea pot interveni și evolua.

**Recunoașterea și calificarea incidentelor**

Pe scurt, pornind de la definiția acestora din cuprinsul GDPR, incidentele de securitate a datelor sunt:

* încălcări de confidențialitate, respectiv cele în care are loc o dezvăluire a datelor cu caracter personal sau accesul neautorizat sau accidental la acestea;
* încălcări de integritate, respectiv cele în care are loc o alterare/ modificare a datelor cu caracter personal; și
* încălcări privind disponibilitatea, respectiv cele în care are loc pierderea datelor cu caracter personal sau în care acestea nu mai sunt disponibile pentru operator.

În practică, un incident se poate încadra simultan în toate cele trei categorii de mai sus sau în orice combinație a acestora. Analiza preliminară a unui eveniment prin raportare la cele trei categorii va facilita procesul operatorilor de calificare a acestuia drept incident. Totodată, această analiză va servi în etapa ulterioară a notificării incidentului către autoritatea de supraveghere, dacă va fi cazul, în condițiile în care formularul impus de autoritate în acest sens cuprinde o secțiune vizând chiar această categorisire.

**Câteva situații particulare și exemple practice**

**Riscuri generate de activitatea angajaților.** Incidentele de securitate nu au întotdeauna o cauză externă. Operatorii de date trebuie să aibă în vedere că și diverse neconformități interne (intenționate sau neintenționate) vor putea fi calificate drept incidente de securitate a datelor. De altfel, aceste ipoteze par a fi din ce în ce mai numeroase, inclusiv prin raportare la [activitatea sancționatorie recentă a ANSPDCP](https://www.dataprotection.ro/?page=allnews). Cu titlu de exemplu, prezentăm în cele ce urmează câteva situații practice relevante:

* un angajat al unei instituții medicale, cu rea-credință, acționând cu încălcarea procedurilor interne, distruge singura copie a unor documente medicale aparținând unor pacienți, situație care va putea reprezenta un incident privind disponibilitatea datelor;
* un angajat al unui operator retail preia, la momentul la care părăsește organizația, o copie a bazei de date conținând informațiile clienților, situație care va putea reprezenta un incident privind confidențialitatea datelor;
* un angajat transmite, din eroare/ neglijență, documente conținând date cu caracter personal către destinatari neautorizați să obțină acces la acestea, cum este cazul e-mailurilor transmise greșit sau chiar intenționat, în alte scopuri decât cele privind îndeplinirea atribuțiilor de serviciu, precum dezvăluirea unor informații către prieteni/ familie, reprezentând tot un posibil incident privind confidențialitatea datelor;
* încălcarea regulilor interne privind distrugerea securizată a documentelor fizice sau generarea diverselor disfuncționalități ale sistemelor ce pot afecta disponibilitatea, integritatea sau confidențialitatea datelor.

**Atacuri cibernetice.** Un caz din ce în ce mai frecvent de incident de securitate experimentat de operatorii de date este cel al atacurilor cibernetice. Deși sunt privite în primă fază ca o problemă de securitate a sistemelor, operatorii trebuie să fie conștienți că, în cele mai multe dintre cazuri, aceste situații vor reprezenta și o problemă de securitate a datelor, pe care vor fi nevoiți să o gestioneze potrivit prevederilor GDPR. Exemple includ:

* atacuri cibernetice vizând criptarea bazei de date de clienți ai operatorului, ce va reprezenta, ca regulă, un incident de disponibilitate;
* atacuri cibernetice în care se reușește exfiltrarea unor informații vizând angajații sau obținerea accesului la conturile de e-mail aparținând unor angajați, ce vor putea fi calificate drept incidente privind confidențialitatea datelor.

**Echipamente pierdute sau furate.** În acest caz, avem în vedere ipoteza în care echipamentele încredințate angajaților pentru îndeplinirea atribuțiilor de serviciu sunt pierdute sau furate. Poate fi astfel vorba, în special, despre echipamentele portabile, cum ar fi laptop-uri, tablete, telefoane sau stick-uri de memorie, care în mod firesc pot conține documente ce cuprind date cu caracter personal sau permit accesul în aplicații în care sunt prelucrate acestea.

Astfel, furtul sau pierderea unor astfel de echipamente va putea reprezenta o problemă de confidențialitate a datelor (în special în cazul în care echipamentele sau fișierele/ aplicațiile relevante nu sunt securizate corespunzător – prin mecanisme de criptate, spre exemplu). Mai mult, poate fi și o problemă de disponibilitate a datelor, în cazul în care, la nivelul organizației nu există back-up corespunzător pentru informațiile disponibile pe echipamente. Din această perspectivă, relevante pot fi chiar și echipamentele personale ale angajaților, în cazul în care acestea sunt utilizate de către ei pentru exercitarea atribuțiilor de serviciu.

**Măsuri recomandabile pentru operatorii de date**

Pe lângă orice măsuri de prevenție existente, operatorii trebuie să fie în măsură să recunoască un potențial incident de securitate a datelor și să identifice impactul asupra protecției datelor, dacă e cazul, prin raportare la oricare dintre scenariile ce pot interveni.

Aceasta implică, în principal, instruirea corespunzătoare a personalului relevant, pe toate fluxurile de prelucrare, pentru ca aceștia să poată identifica preliminar un potențial incident de securitate a datelor, să îl informeze pe responsabilul cu protecția datelor/ alte persoane cu atribuții în acest sens și să coopereze cu aceștia în analiza și gestionarea situației.

În continuare, analiza de risc a incidentului și determinarea obligațiilor de notificare trebuie realizată de la caz la caz, în funcție de caracteristicile concrete ale fiecărei spețe. Aceasta, împreună cu implementarea de măsuri adecvate de răspuns la incident sau pentru adaptarea măsurilor tehnice și organizatorice existe, ce prin apariția incidentului s-au dovedit a nu fi suficiente. Orientări în acest sens oferă și îndrumările emise la nivel european în materia incidentelor de securitate a datelor, cum sunt cele emise de către [Comitetul European pentru Protecția Datelor](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en), de către precursorul său, [Grupul de Lucru Art. 29](https://ec.europa.eu/newsroom/article29/items/612052) sau de către autoritățile de supraveghere din [Irlanda](https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf), [Marea Britanie](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/) și [Spania](https://www.aepd.es/sites/default/files/2019-09/Guide-on-personal-data-breach.pdf).

*Articol scris de: Marta Tudor, Attorney at Law, avocat specializat în protecția datelor cu caracter personal în cadrul Schoenherr și Asociații SCA*