**Metodologia de evaluare a impactului privind protecția datelor (EIPD) conform RGPD al UE**

Modelul de implementare al RGPD al UE Articolul 35 din RGPD al UE oferă un instrument analitic specific de evaluare a impactului GDPR în profunzime, etapă cu etapă.

EIPD este de fapt întruchiparea unui mix de aspecte juridice, de evaluare, tehnice și de comunicare. În plus, include atât procedura de control, cât și cea de procesare de date și asigură responsabilitatea unei companii.

Există o obligație legală de a efectua o evaluare în cazul în care prelucrarea poate duce la un risc ridicat pentru persoana vizată (articolul 35 din RGPD). Având în vedere miza într-o afacere și evoluția sistemelor TI, o abordare de gestionare a riscurilor permite unei organizații să determine controalele necesare. Aceasta face posibilă studierea procesării, prioritizarea riscurilor și tratarea acestora într-un mod proporțional, pentru a optimiza costurile și a lua decizii. În cele din urmă, o metodologie precum EIPD ajută o companie să demonstreze implementarea principiilor de confidențialitate. În consecință, putem admite că un EIPD este un instrument de conformitate; și trebuie utilizat înainte de implementarea procesării.

EIPD constă în mod normal din mai multe etape. Fiecare dintre aceste etape analizează o caracteristică specifică a procesării datelor în comparație cu o serie de controale și verificări. Dacă v-ați întrebat vreodată ce face un pilot și un copilot înainte de a decola, ei parcurg de fapt o listă de verificare a instrumentelor împotriva unei serii de controale reglementate și revizuite. EIPD este similar cu acesta, dar are o oarecare flexibilitate, spre deosebire de lista de verificare a avionului.

EIPD este adaptabilă la profunzimea evaluării care se dorește a fi efectuată, ceea ce înseamnă că nu există un interval de timp indicat pentru fiecare element de evaluare. Cu alte cuvinte, dacă echipa de evaluare dorește să petreacă timp elaborând controale sau să caute și să studieze amenințările la procesare, ar trebui să le lăsați să o facă, deoarece remediile vor fi rezultatul așteptat al acestei analize. În ceea ce privește metodologia, articolul 35.7 din regulament prevede elementele minime care trebuie evaluate, care sunt descrise mai jos în 5 etape:

**Etapa 1** este în esență o listă detaliată a procesării datelor, inclusiv: datele pe care le folosește, detaliile operatorilor și procesatorilor, baza legală sau perioadele de păstrare aplicate datelor.

**Etapa 2** identifică controalele legale și de tratare a riscurilor care sunt implementate în prezent. Această fază implică setul actual și existent de măsuri din punct de vedere juridic, tehnic, fizic și organizațional. Obiectivul este de a controla orice riscuri care pot fi identificate înainte de implementarea procesării datelor. Dacă, de exemplu, o afacere nu și-a revizuit politica privind accesul la sediul său (de exemplu: eliberarea insignelor, jurnale de acces etc.), trebuie să o facă mai întâi înainte de a extinde o astfel de politică într-o zonă nou construită / dobândită a sediului dvs. sau a unui sistem nou.

**Etapa 3** enumeră sursele de risc pentru prelucrarea datelor. Aceasta ridică următoarea întrebare: „va suferi afacerea mea de această nouă prelucrare a datelor și, dacă da, unde și când va suferi?” Această fază se concentrează pe posibile intruziuni ale confidențialității (de exemplu, daune cauzate de date inexacte sau o încălcare a securității) și o evaluare a riscurilor corporative, deteriorarea reputației sau a costurilor financiare. Solicită imaginație, în special pentru a răsfoi o cantitate echitabilă de surse de risc împotriva companiei. Dacă ne referim la o firmă bancară, una dintre sursele de risc este că baza de date ar putea fi compromisă și accesată în mod fraudulos. Este un risc de securitate în sine, dar prezintă și un risc financiar pentru acțiunile companiei, în timp ce prezintă un risc și privind reputația în fața clienților.

**Etapa 4** se referă la analiza și listarea potențialelor evenimente negative și amenințări la procesarea datelor. Distincția sa față de faza 3 este că se va concentra asupra datelor personale ale persoanelor vizate și asupra impactului potențial al noii prelucrări asupra acestor date. În cazul în care evenimentele sunt interne sau externe, umane sau neumane (tehnice), această fază este relevantă în ceea ce privește evoluțiile tehnologice. Este posibil ca noile tehnologii să nu aibă o introducere clară a măsurilor de protecție prietenoase confidențialității și astfel să expună persoanele vizate la amenințări precum hacking, phishing și spam. Scopul său este de a determina la ce tip de amenințări poate fi expusă prelucrarea dvs. Să presupunem că sunteți directorul unui spital mare. Dosarele de sănătate ale pacienților sunt foarte sensibile. O amenințare umană ar fi că aceste înregistrări sunt accesate de membrii personalului greșit dintr-un motiv greșit, iar o amenințare non-umană ar fi că sistemul de operare utilizat de spitalul este cel care funcționează de 10 ani fără actualizări. În prima instanță, poate apărea un acces neautorizat și fraudulos, în timp ce în a doua instanță, poate avea loc un atac cibernetic asupra sistemului de operare. În cele din urmă, secretul medical al pacienților va fi amenințat dacă nu se remediază amenințarea.

În cele din urmă, **etapa 5** are forma unui raport și rezumă analiza, controalele actuale, riscurile pentru afacere și amenințările la adresa datelor personale. Raportul stabilește opțiunile organizației pentru abordarea fiecărui risc identificat, amenințare și defect. Se precizează dacă fiecare opțiune ar duce la eliminarea, reducerea sau acceptarea riscului așa cum este. Raportul va fi înregistrat, păstrat și prezentat managerilor principali ai organizației. Acești manageri pot decide astfel dacă au fost întreprinse acțiuni sau trebuie să fie întreprinse și să urmărească astfel de acțiuni. Putem observa aici că astfel de rapoarte contribuie la conformitatea cu principiul responsabilității al RGPD.

O astfel de evaluare oferă o oportunitate puternică de a revizui documentele, de a pregăti implementarea proiectului, de a vă construi sau adapta politicile, de a actualiza aspectele tehnice și de a vă consolida controalele. Pe scurt, EIPD responsabilizează personalul să facă schimbări și să conștientizeze protecția datelor cu caracter personal în cadrul companiei.

Demonstrarea conformității către autoritățile de protecție a datelor este ceea ce trebuie să fie considerat și trebuie să se țină o evidență a acestora. În cazul unui audit pot fi prezentate aceste înregistrări. În plus, clienții companiei și persoane vizate vor avea garanția privind protecția datelor și reputația.

**Metodologia de evaluare a severității compromiterii datelor cu character personal (ESCDP) conform RGPD al UE**

Metodologia de evaluare a severității încălcărilor de date cu caracter personal, în conformitate cu opiniile grupului de lucru al articolului 29 „Orientări privind notificarea încălcării datelor cu caracter personal în temeiul Regulamentului 2016/679” și „Recomandări pentru o metodologie de evaluare a severității datelor personale încălcări de date” emisă de Agenția Uniunii Europene pentru Securitatea Rețelelor și Informațiilor (ENISA), se bazează și pe evaluarea gravității încălcărilor de date în organizațiile din diferite domenii de activitate și este menită să ofere un model simplu și cuprinzător de evaluare a încălcărilor de date.

Metodologia se bazează pe o abordare obiectivă, încercând în același timp să rămână suficient de flexibilă pentru a fi adoptată de diverse întreprinderi. În funcție de diferite cerințe, punctarea unor categorii poate fi ajustată pentru a produce cele mai adecvate rezultate.

Pentru a evalua severitatea generală a încălcării datelor și pentru a obține un rezultat care va fi ușor de interpretat, se propune următoarea formulă:

**SC = CPD x UI + CC,** unde

**SC** înseamnă **Severitatea compromiterii**,

**CPD** înseamnă **Contextul procesării datelor**,

**UI** înseamnă **Ușurința identificării**,

**CC** înseamnă **Circumstanțe de încălcare**.

***2.4.1. Contextul procesării datelor (CPD)***

CPD abordează tipul de date încălcate, împreună cu o serie de factori legați de contextul general al prelucrării.

CPD evaluează criticitatea unui set de date dat într-un context de procesare specific și poate fi reprezentat cu o valoare de 1, 2 sau 3, în funcție de categoria datelor personale implicate în încălcarea datelor.

La definirea scorului pentru CPD, controlorii ar trebui să ia în considerare următoarele:

- Dacă încălcarea datelor cu caracter personal implică doar categorii nesensibile de date cu caracter personal (cum ar fi numele, prenumele, adresele de e-mail etc.), CPD = 1.

- În cazul în care încălcarea datelor cu caracter personal implică doar categorii nesensibile de date cu caracter personal, dar datele ar putea fi utilizate pentru a înțelege profilul persoanelor vizate afectate (de exemplu, dacă încălcarea datelor conține o listă de clienți de la o companie care vinde produse de lux, apoi se pot face ipoteze cu privire la starea financiară a persoanelor vizate), CPD = 2.

- Dacă încălcarea datelor cu caracter personal implică doar categorii speciale de date cu caracter personal (cum ar fi date referitoare la sănătate, date genetice, condamnări penale, credințe religioase și / sau filosofice etc.), CPD = 3.

***2.4.2. Ușurința de identificare (UI)***

UI reflectă cât de ușor poate fi determinată identitatea persoanelor din datele personale implicate în încălcare.

UI este un factor de corectare al CPD. Criticitatea generală a unei încălcări a datelor poate fi ajustată în funcție de valoarea UI. Evaluează cât de ușor va fi pentru o parte neautorizată care are acces la setul de date să le potrivească cu o anumită persoană vizată. Astfel, produsul UI și CPD oferă scorul inițial al severității (SE) a compromiterii datelor.

UI poate avea o valoare de 1 sau 2 în funcție de tipul de criptare utilizat pentru a proteja datele personale. La definirea scorului pentru UI, controlorii ar trebui să ia în considerare următoarele:

- Dacă datele personale implicate în încălcarea datelor sunt protejate utilizând o criptare puternică (cum ar fi Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Twofish etc.), ceea ce face dificilă identificarea unei persoane vizate, UI = 1.

- Dacă datele cu caracter personal implicate în încălcarea datelor sunt în format text simplu și pot fi asociate în mod specific cu o persoană vizată (de exemplu, datele cu caracter personal implicate în încălcarea datelor constau din nume, prenume, adresă, număr de securitate socială și adresă de e-mail ), UI = 2.

***2.4.3. Circumstanțe de compromitere (CC)***

CC abordează circumstanțele specifice ale compromiterii, care sunt legate de tipul compromiterii, inclusiv în principal pierderea securității datelor încălcate, precum și orice intenție rău intenționată implicată.

CC cuantifică circumstanțele specifice ale compromiterii care pot fi sau nu prezente într-o anumită situație. Deci, atunci când este prezent, CC poate crește doar severitatea unei anumite încălcări.

La calcularea gravității compromiterii datelor, numai una dintre circumstanțele descrise mai jos poate fi luată în considerare pentru fiecare încălcare a datelor:

* Datele personale sunt difuzate către unii destinatari cunoscuți neautorizați, de exemplu, (1) E-mailurile care conțin date personale sunt trimise unor destinatari cunoscuți care nu ar trebui să primească e-mailurile sau (2) Setarea incorectă a permisiunii permite anumitor utilizatori neautorizați să acceseze datele personale ale altora, CC = 1.
* Datele personale sunt transmise către unii destinatari necunoscuți, de exemplu, (1) Datele personale sunt încărcate incorect pe paginile web publice sau (2) Configurarea incorectă permite unui utilizator arbitrar neautorizat să acceseze toate datele personale de pe site, CC = 2.
* Datele cu caracter personal sunt modificate și utilizate incorect sau ilegal, afectând persoanele vizate; cu toate acestea, datele modificate pot fi restaurate, de exemplu, unele parole de cont stocate în sistem sunt modificate. Prin urmare, conturile afectate nu pot fi conectate în mod normal într-o anumită perioadă de timp. Cu toate acestea, datele modificate pot fi restaurate, CC = 1.
* Datele cu caracter personal sunt modificate și utilizate incorect sau ilegal, afectând persoanele vizate. Datele modificate nu pot fi restaurate, de exemplu, unele parole de cont stocate în sistem sunt modificate, iar datele modificate nu pot fi restaurate. Ca urmare, conturile afectate nu mai pot fi conectate, CC = 2.
* Datele personale nu pot fi accesate, dar datele pot fi restaurate, de exemplu, datorită greșelilor personalului de întreținere, conturile utilizatorilor serviciilor online se pierd. Cu toate acestea, conturile pot fi recreate prin alte baze de date, CC = 1.
* Datele personale nu pot fi accesate sau restaurate, de exemplu, baza de date a unui forum este deteriorată și toate activitățile stocate ale utilizatorilor forumului sunt pierdute. Datele pierdute nu au nicio copie de rezervă și nu pot fi furnizate din nou de către utilizatori., CC = 2.
* Încălcările datelor cu caracter personal sunt cauzate de un comportament rău intenționat care afectează în mod negativ persoanele, de exemplu, (1) Angajații partajează datele personale ale clientului pe site-uri web externe, sau (2) Angajații vând datele personale ale clientului către terți, sau (3) Hackerii intră în sistemul IT corporativ și fură date cu caracter personal. ,CC = 2.

***2.4.4. Evaluarea nivelului de severitate a încălcărilor***

În cazul unei încălcări a datelor, compania va evalua toate circumstanțele descrise mai sus și va atribui o valoare corespunzătoare fiecăruia dintre parametrii din formula **SC = CPD x UI + CC**.

După obținerea valorii exacte a severității compromiterii (SC), puteți consulta tabelul de mai jos pentru a verifica impactul asupra persoanelor vizate afectate, consecințele posibile pentru persoanele vizate și obligațiile de notificare ale companiei în cazul unei încălcări a datelor.

|  |  |  |  |
| --- | --- | --- | --- |
| **Valoarea SC** | **Impactul asupra persoanelor vizate afectate** | **Consecințe posibile pentru persoanele vizate** | **Obligația de notificare** |
| SC este mai mic sau egal cu 3 | Este puțin probabil să conducă la un risc | Indivizii fie nu vor fi afectați, fie pot întâmpina câteva inconveniente, pe care le vor depăși fără nicio problemă (timpul petrecut reintroducând informații, supărări, iritații etc.). | Încălcarea datelor trebuie înregistrată numai într-un registru |
| SC = 4 | Este posibil să apară un risc | Persoanele pot întâmpina inconveniente semnificative, pe care le vor putea depăși în ciuda câtorva dificultăți (costuri suplimentare, refuzul accesului la serviciile comerciale, frică, lipsă de înțelegere, stres, afecțiuni fizice minore etc.). | Încălcarea datelor ar trebui raportată autorității de supraveghere. |
| SC este mai mare sau egal cu 5 | Foarte probabil să conducă la risc | Persoanele pot întâmpina consecințe semnificative, sau chiar ireversibile, care se pot dovedi dificile sau imposibil de depășit (deturnare de fonduri, listă neagră de către bănci, daune materiale, pierderea locurilor de muncă, citație, agravarea stării de sănătate, suferință financiară, cum ar fi datorii substanțiale sau incapacitate de muncă , afecțiuni psihologice sau fizice pe termen lung, deces etc.). | Încălcarea datelor ar trebui raportată autorității de supraveghere, precum și persoanelor vizate afectate. |

Deși obligațiile de notificare solicitate de GDPR UE pot părea destul de simple, în practică, multe scenarii de încălcare nu sunt clare și necesita o evaluare atentă de la caz la caz. Metodologia oferă o abordare comună în ceea ce privește asigurarea responsabilității și conformității cu prevederile RGPD al UE privind notificarea compromiterii datelor și permite operatorilor să aibă o abordare clară atunci când evaluează gravitatea încălcărilor datelor cu caracter personal. Evaluarea corectă a compromiterii trebuie analizată cu atenție de către controlori, deoarece o nereușită pe această linie ar putea pune în discuție conformitatea companiei cu RGPD al UE.

Evaluarea corectă a unei încălcări a datelor este esențială în lumina noilor sancțiuni care vor fi aplicate de autoritățile de supraveghere, pentru faptul că nu se notifică încălcarea datelor, după cum este necesar, poate duce la amenzi administrative de până la 10.000.000 EUR sau, în cazul unei întreprindere, până la 2% din totalul cifrei de afaceri anuale mondiale din exercițiul financiar precedent.

În cele din urmă, chiar dacă RGPD al UE solicită operatorilor doar să notifice încălcările de date, dacă procesatorii devin conștienți de o încălcare a datelor, aceștia trebuie să notifice operatorul fără întârzieri nejustificate pentru a permite operatorului să își respecte obligațiile de notificare.