Măsuri tehnice necesare pentru alinierea la GDPR

avocat
Alexandru Matei
Associate SĂVESCU & ASOCIAŢII

Vlad Bercu
Research assistant
SĂVESCU & ASOCIAŢII

Necesitatea adoptării de măsuri de securitate de către operatorii care prelucrează date cu caracter personal care, în activitatea lor folosesc softuri, derivă dintr-o obligație generală a operatorilor pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu GDPR. Respectivele măsuri se revizuiesc și se actualizează dacă este necesar. Există câteva aspecte esențiale care trebuie avute în vedere, astfel încât cerințele de securitate ale software-ului să fie conforme cu GDPR.

1. Înțelegerea modului în care GDPR afectează compania prin efectuarea unei evaluări de impact asupra protecției datelor (art. 35 GDPR). Evaluarea măsurilor avute în vedere pentru prevenirea riscurilor, incluzând măsuri și mecanisme de securitate. Pentru conformitatea cu art. 35 GDPR ar trebui efectuată o analiză comparativă de natură a furniza o perspectivă obiectivă asupra securității softului și gradului de conformitate al operațiunilor – oferind o vizibilitate măsurabilă în zonele care ar putea beneficia de îmbunătățiri. De asemenea, se impune și adoptarea unei strategii de apărare în cazul producerii unui incident, strategie adresată securității și nevoilor calitative și specifice companiei, astfel încât să fie eliminate vulnerabilitățile și prevenirea problemelor înainte ca acestea să apară.

2. Cunoașterea obligațiilor companiei din perspectiva GDPR. Acest lucru presupune:

– păstrarea evidenței tuturor activităților de prelucrare a datelor cu caracter personal, precum și motivele care stau la baza lor;

– efectuarea evaluării de impact pentru măsurarea riscului confidențialității datelor și evaluarea măsurilor și mecanismelor instituite pentru securitatea datelor înainte ca acestea să fie prelucrate (art. 35 GDPR);

– examinarea evaluării efectuate pentru a stabili dacă procesarea standardelor de securitate poate evolua odată cu riscurile; punerea în aplicare de măsuri privind confidențialitatea datelor prin proiectare (în funcție de sensibilitatea datelor) – adică integrarea protecției datelor și a vieții private chiar din momentul proiectării noilor produse, servicii și proceduri care implică prelucrarea datelor cu caracter personal;

– respectarea noilor cerințe de transparență, de legalitate a prelucrării și notificarea persoanelor cu privire la drepturile lor; în cazul unui incident de securitate, notificarea autorității de supraveghere și a persoanelor vizate afectate în termen de 72 de ore (articolul 33 GDPR);

– desemnarea unui responsabil cu protecția datelor (DPO), acolo unde este cazul (art. 37 GDPR).

3. Stabilirea calității în care acționează compania, dacă aceasta este un operator sau o persoană împuternicită (procesator de date). Operatorii trebuie să aibă certitudinea că datele sunt prelucrate într-un cadru securizat, fie prin propria companie, fie de către un procesator de date terță parte. Împuterniciții (procesatorii) trebuie să dispună de măsuri adecvate de securitate tehnică. De exemplu, o implementare ISO

27001 ar fi un bun început. Securitatea software-ului, a rețelei și mediilor este esențială. Cel mai bun mod de a crea o cultură de securitate a software-ului într-o companie este de a pune în aplicare o inițiativă de securitate software.

4. Obținerea sprijinului din partea managementului superior al companiei, eventual, prin evidențierea potențialelor amenzi corelată cu propunerea unei strategii viabile pentru îndeplinirea obligațiilor cu care compania se confruntă.

5. Desemnarea unui responsabil cu protecția datelor. Un aspect important pe care rolul de DPO îl implică este asigurarea securității oricărei părți a software-ului care joacă un rol important în prelucrarea datelor cu caracter personal. El trebuie, de asemenea, să se asigure de monitorizarea continuă în scopul identificării noilor vulnerabilități ce afectează aplicațiile de producție (cele la care au acces direct utilizatorii).

6. Implementarea mecanismelor tehnice în interiorul softului care asigură securitatea și confidențialitatea datelor cu caracter personal. Securitatea trebuie construită în soft și sistemele prin care datele cu caracter personal trec, de la început, conform standardelor și practicilor documentate pentru a minimiza suprafața de atac. Art. 25 GDPR prevede instituirea de măsuri pentru a se asigura că datele cu caracter personal nu sunt făcute accesibile fără consimțământul persoanei (inclusiv în timpul unui incident). În cele din urmă, defectele de arhitectură ale aplicațiilor sunt, prin însăși natura lor, provocările cu cel mai mare impact asupra securității și confidențialității datelor. Din fericire, identificarea lor înainte de implementarea unui sistem previne operațiunile destul de costisitoare, cum ar fi reluarea de la zero a unui întreg proces sau fixarea acelor defecte. Cu toate acestea, nu există limite de identificare a defectelor înainte ca implementarea să fie afectată. Acest lucru se poate întâmpla numai în stadiul inițial al unei dezvoltări, precum și în cazul adăugării unor module noi unui software existent. Cel mai des întâlnit scenariu este identificarea unei erori într-un sistem existent ca urmare a analizei riscului de arhitectură. În acest caz este foarte important să fie evaluate opțiunile pentru a elimina sau a diminua efectele acelei erori. O soluție temporară poate fi implementată pe un sistem la care au deja acces utilizatorii, în timp ce arhitecții vor lucra pentru o soluție finală, cu scopul de a elimina complet eroarea.

7. În ceea ce privește evoluția pieței software-urilor pentru ca companiile să își accelereze traseul către conformitatea cu noile standarde GDPR, giganții precum IBM și Microsoft deja oferă un produs calitativ. IBM vine cu un soft denumit IBM Spectrum Data Protection, care, conform descrierii, simplifică administrarea backup-urilor, face mai ușor administrarea bazelor de date pentru operator, garantează un nivel sporit al protecției datelor persoanelor vizate. Mai mult, tot mai des se discută despre implementarea tehnologiei blockchain în cadrul prelucrării datelor cu caracter personal, care ar garanta într-o măsură mai mare protecția identității persoanelor vizate și securitatea datelor, împotriva ștergerii și modificării neautorizate a acestora.