SUNTEM GATA?

Implementarea Regulamentului General privind Protecția Datelor cu Caracter Personal

Alexandru Ambrozie
Avocat Asociat
Popovici Nițu Stoica & Asociații

Ana Stoenescu
Avocat Colaborator
Popovici Nițu Stoica & Asociații

GDPR, NIS, PSD 2 – pentru majoritatea oamenilor reprezintă doar litere, dar pentru bănci reprezintă schimbările anului 2018 pregătite de Uniunea Europeană. Directivele și regulamentele adoptate în urmă cu doi ani vor intra în vigoare, iar ultima sută de metri se poate dovedi esențială în implementarea noilor obligații.

Cu siguranță, un punct comun al celor trei acte europene (GDPR - Regulamentul General privind Protecția Datelor cu Caracter Personal; NIS - Directiva privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice; PSD II - Directiva privind serviciile de plată) îl constituie protecția datelor cu caracter personal.

GDPR - Amenințări?

Întrucât băncile prelucrează constant date cu caracter personal, acestea sunt direct vizate de noile prevederi din GDPR care vor intra în vigoare la 25 mai 2018.

Pentru a asigura respectarea obligațiilor, GDPR prevede amenzi foarte ridicate, care ajung rapid la 10 până la 20 milioane de euro sau între 2% și 4% din cifra de afaceri mondială totală anuală. Totuși, amenzile și controalele efectuate de autoritatea de supraveghere, care va avea puteri extinse, nu reprezintă singura problema a băncilor. Neconformarea cu dispozițiile GDPR poate impacta reputația unei bănci, iar încrederea oferită clienților constituie un principiu de bază al sistemului bancar.

Toate acestea, cu atât mai mult cu cât în noul context băncile nu mai reprezintă singura sursă de servicii financiare, existând companiile Fintech sau IFNurile, care reprezintă o competiție din ce în ce mai puternică a pieței bancare tradiționale și cărora le poate fi mai ușor să implementeze obligațiile prevăzute de noul Regulament.

GDPR – Schimbări?

În lipsa unui contract care să legitimeze prelucrarea datelor cu caracter personal, băncile vor trebui să obțină consimțământul expres al persoanelor vizate (e.g. clienți, angajați) pentru fiecare prelucrare efectuată. Mai mult, va trebui asigurat un mecanism de retragere a consimțământului disponibil în orice moment și care nu poate fi mai complicat decât cel utilizat pentru obținerea acestuia.

Demersul GDPR de a asigura o protecție sporită a datelor cu caracter personal prin introducerea unor noi drepturi ale persoanelor vizate se reflectă și în obligațiile corelative ale operatorilor de date cu caracter personal. Astfel, băncile vor trebui să permită portabilitatea datelor, cerință prevăzută și de PSD II, și ștergerea tuturor datelor cu privire la o persoană vizată, în anumite cazuri expres reglementate.

O atenție sporită trebuie acordată și obligației de notificare a autorității de supraveghere și a persoanelor vizate cu privire la încălcarea securității datelor cu caracter personal, care constituie un aspect comun al

GDPR și NIS. Vor trebui adoptate măsuri tehnice și organizatorice adecvate pentru a putea identifica, controla și ulterior raporta încălcarea securității datelor, fapt frecvent de altfel în contextul actual și sub presiunea atacurilor cibernetice.

În plus, este necesară numirea unui responsabil cu protecția datelor care va coordona activitatea de prelucrare, va reprezenta punctul de contact atât pentru autoritatea de supraveghere, cât și pentru persoanele vizate și va asista banca în toate demersurile privitoare la respectarea obligațiilor impuse de GDPR. Responsabilul cu protecția datelor va furniza consiliere și pentru efectuarea evaluărilor impactului asupra protecției datelor, evaluări efectuate anterior prelucrării datelor cu caracter personal și care vor evidenția riscurile pentru drepturile persoanelor vizate și posibilitățile de diminuare ale acestora.

Obligația de a notifica autoritatea de supraveghere nu mai este prevăzută de GDPR, însă beneficiul aparent al acestei eliminări vine împreună cu introducerea obligațiilor de efectuare a unei evaluări a impactului asupra protecției datelor și de numire a unui responsabil cu protecția datelor, obligații pentru care operatorul de date cu caracter personal va fi pe deplin răspunzător.

GDPR – Soluții?

Cu toate acestea, schimbările aduse în domeniul protecției datelor cu caracter personal nu ar trebui privite drept obligații, ci oportunități pentru a îmbunătăți structura organizațională a băncii, a actualiza datele cu caracter personal stocate, a implementa noi tehnologii, a obține consimțământul clienților, a-i informa cu privire la noile obligații și în mod special a întări relația cu aceștia.

Startul pentru implementarea GDPR s-a dat în anul 2016; schimbările pot fi încă integrate, iar amenințările prevenite până în mai 2018, însă procesul de conformare trebuie început de îndată.