

Efectul caderii mecanismului EU-US Privacy Shield – pe cine afectează și ce alternative au companiile vizate



Hotărârea Curții de Justiție a Uniunii Europene (CJUE), prin care a declarat nul acordul care permitea transferul de date cu caracter personal între Uniunea Europeană (UE) și Statele Unite ale Americii (SUA), denumit *EU-US Privacy Shield*, a creat îngrijorare atât în rândul specialiștilor pe teme de protecția datelor cu caracter personal, dar mai ales printre companiile multinaționale. Este vorba în principal de companiile care transfera datele către societățile mama, sau de cele care utilizează serviciile unor companii americane, precum furnizorii de servicii de tip *cloud*.

Însă, înainte de a evalua impactul pe care acest eveniment îl are asupra activității companiilor vizate, trebuie punctate câteva aspecte.

În ce a constat mecanismul *EU-US Privacy Shield*?

Programul permitea companiilor americane să se înscrie pe site-ul Departamentului de Comerț al Statelor Unite și să auto-certifice aderarea la cadrul *Privacy Shield* și îndeplinirea cerințelor adecvate legate de protecția datelor cu caracter personal. Aderarea la acest program facilita transferul datelor cetățenilor UE către companiile americane și oferea încredere partenerilor și autorităților din UE, responsabile cu protecția datelor cu caracter personal, ca datele europenilor sunt prelucrate în conformitate cu cerințele GDPR.

Alternative la programul *EU-US Privacy Shield*

Este important de menționat că nu toate transferurile de date cu caracter personal către SUA se realizau în baza programului *EU-US Privacy Shield*. Există companii care fie nu au aderat la acest cadru, fie au considerat mai potrivite celelalte opțiuni pe care le pune la dispoziție GDPR.

• Unele din alternativele la mecanismul oferit de *Privacy Shield* constă în utilizarea **regulilor corporatiste obligatorii (*Binding Corporate Rules*)**, un cod de reguli dezvoltat de către companie și validat de autoritățile responsabile cu protecția datelor cu caracter personal. În baza acestor reguli, datele cu caracter personal pot fi transferate către țări din afara UE. Principalul dezavantaj al utilizării regulilor corporatiste obligatorii este că se aplică doar transferurilor operate în cadrul aceluiași grup de companii, neputând fi utilizate în relația client – furnizor.

• Utilizarea **clauzelor contractuale standard adoptate de Comisia Europeană** este, probabil, cea mai utilizată opțiune pentru demonstrarea caracterului adecvat al măsurilor de protecție a datelor cu caracter personal, constând într-un set de prevederi care se încheie ca o anexă separată în relațiile comerciale cu companiile

americane. Acestea sunt disponibile companiilor pe site-ul Comisiei Europene. Prin decizia luata joi, 16 iulie, se menține aceasta opțiune pentru transferul datelor catre SUA.

Pe lângă cele doua alternative descrise mai sus, GDPR prevede și alte modalități adecvate pentru realizarea transferurilor de date, mai greu de implementat în prezent, dar a caror exploatare este de așteptat sa creasca în viitorul apropiat.

Printre acestea se numara:

- utilizarea unor clauze contractuale între părți, care nu necesita aprobarea Comisiei, dar trebuie autorizate de Autoritatea de Protecția Datelor competenta;
- utilizarea clauzelor standard emise de Autoritatea de Supraveghere competenta și aprobate de Comisia Europeana;
- utilizarea unui cod de conduita aprobat de Autoritatea de Supraveghere competenta;
- certificarea companiei americane în conformitate cu mecanismele aprobate, existente la nivelul statului membru UE.

Impactul deciziei CJUE asupra companiilor

Singurele companii afectate de decizia Curții Europene de Justiție sunt cele care transferau date cu caracter personal în baza *EU-US Privacy Shield*. În aceste cazuri, ca urmare a deciziei curții, se impune evaluarea transferurilor realizate și implementarea de urgență a uneia dintre alternativele menționate.

Decizia CJUE a produs, probabil, îngrijorare mai cu seama în rândul utilizatorilor de servicii de tip *cloud*. În ceea ce privește furnizorii din aceasta categorie, încă din 2018 (anul intrării în vigoare a GDPR), aceștia au luat masuri pentru a soluționa problema transferurilor de date cu caracter personal. Printre altele, în contractele încheiate cu furnizorii de servicii de tip *cloud*, s-a inclus o garanție referitoare la stocarea datelor cetățenilor pe teritoriul UE.

În concluzie, deși decizia CJUE are un impact în zona de transfer a datelor cu caracter personal, companiile afectate au la dispoziție alternative viabile pentru a-și continua activitatea în condiții de siguranță a datelor și cu respectarea reglementarilor aplicabile.