TUCA ZBARCEA
ASOCIATII

20 iulie 2020

Buletin Legislativ

Protecția datelor

Sumar:

Invalidarea Privacy Shield UE-SUA. Implicații practice asupra organizațiilor

Pe 16 iulie, CJUE a pronunțat hotărârea *Schrems II* care invalidează decizia privind Scutul de Confidențialitate (Privacy Shield) și oferă clarificări asupra Clauzelor Contractuale Standard (CCS).

Mult zgomot și „ceață" în rândul organizațiilor, în special asupra efectelor hotărârii *Schrems II*. Urmează ca autoritățile de supraveghere din UE și EDPB să reacționeze în curând și să aducă mai multă lumină privind acest subiect.

Până atunci, redăm mai jos câteva aspecte cheie pe care ar trebui să le luați în considerare.

1. Ce înseamnă că Privacy Shield UE-SUA a fost invalidat?

Privacy Shield UE-SUA a permis organizațiilor UE să exporte date către organizații din SUA, enumerate în Lista Privacy Shield UE-SUA. Privacy Shield UE-SUA a fost emis în baza articolului 45 din GDPR, care conferă Comisiei dreptul de a decide că anumite state terțe sau teritorii asigură un nivel de protecție adecvat pentru persoanele vizate și, prin urmare, organizațiilor li se permite să transfere date în astfel de state sau teritorii.

Prin articolul 1 alineatul (1) din Decizia privind Privacy Shield, Comisia a constatat că SUA asigură un nivel de protecție adecvat al datelor cu caracter personal transferate din UE către organizații din SUA pe baza Privacy Shield UE-SUA.

Prin hotărârea *Schrems II*, CJUE a constatat că, dimpotrivă, SUA nu asigură un nivel de protecție adecvat (echivalent cu cel asigurat de țările UE) și, prin urmare, a stabilit că decizia Comisiei privind Privacy Shield UE-SUA este invalidă.

Aceasta presupune că **organizațiile UE nu ar mai trebui să se bazeze pe Privacy Shield UE-SUA pentru transferul de date către organizații din SUA**.

2. Ce se întâmplă cu transferurile în curs de desfășurare în baza Privacy Shield UE-SUA?

CJUE a fost destul de directă pe acest subiect extrem de sensibil și a statuat că organizațiile ar trebui să utilizeze mijloacele alternative de transfer de date prevăzute de articolul 49 din GDPR.

Important de menționat, Secretarul comerțului din SUA, Wilbur Ross, a declarat în 16 iulie 2020 că Departamentul de Comerț al SUA va continua să gestioneze programul Privacy Shield și, în particular, va continua să proceseze cererile de înregistrare (pe bază de auto-certificare) în Privacy Shield.

Deși este destul de devreme să tragem concluzii, cu excepția cazului în care Comisia va adopta o nouă decizie privind nivelul de protecție adecvat oferit de SUA, cel mai probabil Privacy Shield UE-SUA își va încheia în curând existența.

În viitorul apropiat, ne așteptăm ca autoritățile de supraveghere a UE și EDPB să emită poziții (comune) și îndrumări suplimentare către organizații de a nu (mai) utiliza Privacy Shield UE-SUA și de a încerca să se bazeze pe mijloace alternative valabile de transfer de date.

3. Există vreo perioadă de grație pentru conformare în ceea ce privește transferurile în curs în temeiul Privacy Shield UE-SUA?

Nu. Organizațiile ar trebui să ia în considerare imediat mijloace alternative valide pentru transferul de date în SUA. Acestea ar putea consta fie în punerea în aplicare a CCS adecvate sau a regulilor corporative obligatorii - RCO (fezabilitatea de evaluat de la caz la caz) sau utilizarea oricăruia dintre mecanismele alternative de transfer descrise la articolul 49 din GDPR.

4. Sunt clauzele contractuale standard (CCS) în continuare valide?

În principiu, da. Totuși, principala provocare va fi ca organizațiile UE care exportă datele în țări terțe în baza CCS să poată demonstra că importatorul de date din țara terță este **în fapt** capabil să îndeplinească garanțiile stipulate în cadrul CCS. Acest lucru ar presupune că organizațiile care se bazează pe CCS verifică dacă legislația țării terțe asigură un nivel similar de protecție în conformitate cu legislația UE în ceea ce privește drepturile persoanelor vizate.

5. La ce ar trebui să se aștepte organizațiile pe viitor?

În primul rând, organizațiile ar trebui să se aștepte **la o creștere semnificativă a numărului de solicitări de acces ale persoanelor vizate viz**ând transferurile de date către țări terțe. Putem presupune în mod rezonabil că cele mai expuse industrii vor fi telecomunicațiile, industria financiar-bancară, asigurările, sănătatea, retail etc.

În mod corespunzător, anticipăm **o creștere a numărului de reclamații ale persoanelor vizate și, în acest sens, a investigațiilor** inițiate de autoritățile UE (inclusiv ANSPDCP) în legătură cu transferurile de date către țări terțe (indiferent dacă sunt făcute pe baza Privacy Shield UE-SUA, CCS sau RCO).

De asemenea, nu putem exclude ca autoritățile naționale să deschidă **investigații din oficiu cu privire la validitatea mecanismelor de transfer** de date utilizate de organizații, cu accent pe transferurile de date către țări terțe. În special, unele autorități de supraveghere ale UE au subliniat deja necesitatea unei abordări unitare în ceea ce privește deciziile pe care le vor lua în privința companiilor care transferă date în țări terțe[1].

Însă, probabil cel mai dramatic impact pentru organizații este că, în conformitate cu articolului 58 din GDPR, autoritățile de supraveghere din UE (inclusiv ANSPDCP) vor putea interzice (temporar sau definitiv) sau ordona suspendarea unui transfer de date sau a unui set de transferuri bazate pe CCS, dacă constată că transferul ar putea să aibă un efect negativ semnificativ asupra garanțiilor oferite persoanei vizate (inclusiv în cazul în care s-ar constata că, în fapt, legislația importatorului de date îl împiedică să se conformeze cu garanțiile oferite formal prin CCS).

În sfârșit, din perspectiva cadrului de conformare, cel mai probabil Comisia va emite versiuni actualizate ale CCS[2]. Este de așteptat ca aceste versiuni să includă mecanisme mai dure pentru asigurarea unei protecții adecvate și eficiente a persoanelor vizate și, cel mai probabil, organizațiile vor fi obligate să încheie noi CCS pe modelul acestor versiuni actualizate.

6. Ce ar trebui să facă organizațiile în continuare?

Puteți lua în considerare următorii pași:

a. **Identificați urgent și țineți o evidență** a tuturor transferurilor către țări terțe pentru care v-ați bazat pe Privacy Shield UE-SUA, CCS or RCO.

b. Pentru transferurile **către SUA**:

i. **Suspendați sau încetați temporar** orice transfer de date pe baza Privacy Shield UE-SUA. Monitorizați îndeaproape orice evoluție pe această temă, în special emiterea de către Comisie a unei noi decizii privind asigurarea unui nivel de protecția adecvat de către SUA.

---

[1] A se vedea comunicatul emis de autoritatea de protecție a datelor din Germania HmbBfDI - https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/paukenschlag-eugh-schreddert-den-privacy-shield-datenuebermittlung-in-staaten-jenseits-der-eu-aber/.

[2] În observațiile introductive cu privire la hotărârea CJUE *Schrems II*, comisarul Reynders a subliniat că *„lucrăm deja de ceva timp la modernizarea [CCS] și la asigurarea că setul nostru de instrumente pentru transferurile internaționale de date este potrivit scopului. [...] Acum suntem într-un stadiu avansat al acestui proiect și vom ține cont, desigur, de cerințele hotărârii”* - a se vedea https://ec.europa.eu/commission/presscorner/detail/en/statement_20_1366.

ii. **Identificați mecanisme alternative de transfer** conform GDPR, precum CCS, RCO sau derogările enumerate la articolul 49 din GDPR.

iii. Dacă nicio variantă dintre cele de mai sus nu este posibilă, **evaluați impactul asupra afacerii** care rezultă din încetarea acestor transferuri de date imediat și analizați opțiuni alternative (cum ar fi mutarea bazei de date în UE sau într-o țară terță recunoscută ca asigurând un nivel de protecție adecvat).

c. Pentru transferurile de date către **țări terțe altele decât SUA desfășurate în baza CCS**:

i. **Evaluați dacă legislația țării terțe asigură un nivel similar de protecție ca și legislația UE.** *Inter alia*, ar trebui să verificați garanțiile legale legate de orice acces potențial la date al autorităților publice din țara terță și capacitatea reală a importatorului de date de a respecta angajamentele din CCS.

ii. Dacă nu este cazul, ar trebui să luați în considerare următoarele:

- ✓ Verificați dacă **țara terță beneficiază de o decizie privind recunoașterea unui nivel de protecție adecvat** emisă de Comisie. Dacă există o astfel de decizie, **inițiați negocieri pentru încetarea CCS și bazați-vă în continuare pe această decizie privind nivelul de protecție adecvat**.
- ✓ În cazul în care nu există nicio decizie privind nivelul de protecție adecvat, puteți lua în considerare punerea în aplicare a unor garanții suplimentare CCS pentru a face eficientă protecția persoanelor vizate.
- ✓ Dacă nu sunt disponibile sau fezabile garanții suplimentare**, puteți lua în considerare încetarea CCS și aplicare unor mecanisme alternative de transfer valabile în conformitate cu GDPR (cum ar fi RCO sau una dintre derogările enumerate la articolul 49 GDPR).**
- ✓ Dacă nicio variantă dintre cele de mai sus nu este posibilă, **evaluați impactul asupra afacerii** care rezultă din încetarea imediată a acestor transferuri de date către țara terță și **evaluați opțiunile alternative** (cum ar fi mutarea bazei de date în UE sau într-o țară terță recunoscută ca asigurând un nivel de protecție adecvat).

d. **Revizuiți documentele de informare utilizate** (politici de confidențialitate, note de informare etc.) pentru a vă asigura că respectați toate cerințele de

transparență impuse de GDPR în ceea ce privește transferurile de date către țări terțe.

e. **Pregătiți un plan de acțiune** și **prezentați-l managementului** organizației.

f. **Documentați toți pașii** pentru a vă asigura că puteți dovedi că ați pus în aplicare controale eficiente pentru a respecta GDPR și noul cadru stabilit de hotărârea CJUE *Schrems II*.

ciprian.timofte@tuca.ro

Editori

Țuca Zbârcea & Asociații are o experiență vastă în oferirea de consultanță juridică în domeniul **protecției datelor cu caracter personal** unor societăți de top din România și/sau din străinătate active în diverse sectoare comerciale, cum ar fi: medicină, farmacie, IT, industria alimentară, industria mobilei, telecomunicații, servicii financiare etc. Serviciile noastre acoperă toate aspectele legate de protecția datelor cu caracter personal, de la notificarea autorității locale de reglementare (Autoritatea Națională pentru Supravegherea Datelor cu Caracter Personal – **„ANSPDCP"**) cu privire la diverse aspecte (precum notificarea încălcărilor obligațiilor de protecție a datelor cu caracter personal, consultanță în vederea evaluării impactului în ceea ce privește protecția datelor în cazurile cu risc ridicat, consultanță în ceea ce privește evaluările interesului legitim în situații sensibile, etc.), până la realizarea unor analize complexe pe probleme sensibile din domeniul protecției datelor cu caracter personal / RGPD, cum ar fi: implementarea completă a RGPD; realizarea unor evaluări ale impactului asupra protecției datelor (DPIA) și evaluări ale intereselor legitime (LIA); monitorizarea salariaților; geolocație; istoricul apelurilor; fișiere de tip *cookie*; prelucrarea datelor de trafic; implementarea soluțiilor de *cloud computing;* auditarea persoanelor împuternicite să prelucreze datele cu caracter personal; partajarea datelor cu caracter personal; negocierea termenilor relevanți ai contractelor de prelucrare a datelor (CPD); codurile de conduită din industrie; traininguri RGPD/ protecția datelor; soluționarea plângerilor depuse de persoanele vizate, etc. Cei interesați de noutățile din acest domeniu pot accesa și blogul Țuca Zbârcea & Asociații – *dataprivacyblog.tuca.ro*.

Ciprian Timofte
Avocat asociat
+40 374 136 341
ciprian.timofte@tuca.ro

TUCA ZBARCEA
ASOCIATII

Șos. Nicolae Titulescu nr. 4-8
America House, Aripa de Vest, et. 8
Sector 1, 011141, București, România
T + 4 021 204 88 90
F + 4 021 204 88 99
E office@tuca.ro
www.tuca.ro