AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Sumar executiv al opiniei Autorității Europene pentru Protecția Datelor privind decizia de adecvare a proiectului preliminar Privacy Shield UE-SUA

[Textul integral al prezentului aviz poate fi consultat în EN, FR și DE pe site-ul AEPD www.edps.europa.eu]

(2016/C 257/05)

Fluxul de date este global. UE este obligată prin tratate și Carta drepturilor fundamentale a Uniunii Europene, care protejează toate persoanele din UE. UE este obligată să ia toate măsurile necesare pentru a asigura respectarea dreptului la confidențialitate și protecția datelor cu caracter personal, pe parcursul tuturor operațiunilor de procesare, inclusiv al transferurilor.

De la dezvăluirea în 2013 a activităților de supraveghere, UE și partenerul său strategic Statele Unite au căutat să definească un nou set de standarde, în baza unui sistem cu declarații de conformitate, pentru transferul din UE în SUA al datelor cu caracter personal, în scopuri comerciale. La fel ca autoritățile naționale responsabile cu protecția datelor, în era fluxului de date global, instantaneu și imprevizibil, AEPD recunoaște valoarea unui cadru legal sustenabil pentru transferurile comerciale de date între UE și SUA, care reprezintă cel mai mare parteneriat comercial din lume. Însă acest cadru trebuie să reflecte integral valorile democratice comune și individuale, bazate pe drepturi, care sunt exprimate din partea UE în Tratatul de la Lisabona și în Carta drepturilor fundamentale și din partea SUA în Constituția SUA.

Proiectul preliminar Privacy Shield poate fi un pas în direcția corectă, însă formularea actuală nu include în mod adecvat, din punctul nostru de vedere, toate precauțiile corespunzătoare pentru protejarea drepturilor UE ale individului la confidențialitate și protecția datelor cu caracter personal, inclusiv în ceea ce privește compensațiile judiciare. Sunt necesare îmbunătățiri semnificative în cazul în care Comisia Europeană dorește să adopte o decizie de adecvare. În mod special, UE ar trebui să primească reasigurări suplimentare în ceea ce privește necesitatea și proporționalitatea, în locul legitimizării accesului de rutină la datele transferate de autoritățile SUA în baza criteriilor cu bază juridică în țara de destinație, însă nu ca atare în UE, așa cum afirmă tratatele, deciziile UE și tradițiile constituționale comune statelor membre.

Mai mult, într-o epocă a hiperconectivității ridicate și a rețelelor distribuite, declarațiile de conformitate emise de organizațiile private, precum și declarațiile și angajamentele oficialilor publici pot juca un rol pe termen scurt, în timp ce pe termen lung nu ar fi suficiente pentru a proteja drepturile și interesele persoanelor și a satisface integral cerințele unei lumi digitale globalizate, unde multe țări sunt acum echipate cu regulamente de protecție a datelor.

De aceea, o soluție pe termen mai lung ar fi binevenită în dialogul transatlantic, pentru a adopta în legislația federală obligatorie cel puțin principalele principii ale drepturilor ce trebuie identificate clar și concis, așa cum este cazul altor țări non-UE care au fost „strict evaluate" pentru asigurarea unui nivel adecvat de protecție; ceea ce CJUE a exprimat în sentința dată în cauza Schrems prin „esențial echivalent" standardelor aplicabile conform legislației UE și care, în conformitate cu Grupul de lucru „Articolul 29" înseamnă că include „esența principiilor fundamentale" privind protecția datelor cu caracter personal.

Remarcăm în mod pozitiv transparența sporită de care au dat dovadă autoritățile SUA în ceea ce privește folosirea excepțiilor de la principiile Privacy Shield, în scopul aplicării legii, securității naționale și al interesului public.

Însă, în timp ce Decizia privind „sfera de siguranță" considera anterior accesul pentru securitatea națională ca fiind o excepție, atenția dedicată proiectului de decizie Privacy Shield pentru accesarea, filtrarea și analizarea de către poliție sau serviciile de informații a datelor cu caracter personal transferate în scop comercial indică posibilitatea ca excepția să fi devenit regulă. În special, AEPD menționează din proiectul de decizie și anexele sale că, neținând seama de tendințele recente de a trece de la supravegherea fără discriminare pe bază generală către abordări mai țintite și selectate, scara sistemului de colectare a informațiilor și volumul de date transferat din UE, făcând subiectul posibilei colectări și folosiri odată transferate și în mod notabil în timpul tranzitului, poate fi încă ridicată, putând fi pusă sub semnul întrebării.

Deși aceste practici pot fi de asemenea legate de serviciile de informații din alte țări și chiar dacă salutăm transparența autorităților SUA în ceea ce privește această nouă realitate, proiectul de decizie din prezent poate conferi legitimitate acestei rutine. De aceea, încurajăm Comisia Europeană să transmită un semnal mai puternic: date fiind obligațiile ce îi

revin UE conform Tratatului de la Lisabona, accesul și folosirea de către autoritățile publice a datelor transferate în scopuri comerciale, inclusiv în tranzit, ar trebui să aibă loc în situații excepționale și acolo unde acest lucru este indispensabil pentru scopurile specificate de interes public.

În ceea ce privește prevederile pentru transferurile în scop comercial, nu se așteaptă de la operatori să schimbe constant modelele de conformitate. Și totuși proiectul de decizie a fost clasificat în cadrul legal existent al UE, care va fi anulat de Regulamentul (UE) 2016/679 (Regulamentul general privind protecția datelor) din mai 2018, la mai puțin de un an de la implementarea integrală a Privacy Shield de către operatori. RPGD creează și consolidează obligațiile pentru operatori, care depășesc cele nouă principii dezvoltate în Privacy Shield. Indiferent de eventualele modificări finale aduse proiectului preliminar, recomandăm Comisiei Europene să evalueze în mod extins perspectivele viitoare de la primul raport, pentru a identifica la timp etapele relevante pentru soluțiile pe termen mai lung, cu scopul înlocuirii Privacy Shield, dacă este cazul, cu cadre legale mai robuste și mai stabile, în vederea amplificării relațiilor transatlantice.

De aceea, AEPD emite recomandări specifice privind Privacy Shield.

I. **Introducere**

La data de 6 octombrie 2015, Curtea de Justiție a Uniunii Europene (denumită în continuare: CJUE) a anulat ([1]) Decizia privind caracterul adecvat al Sferei de siguranță ([2]). Comisia Europeană a ajuns la un acord politic cu SUA la data de 2 februarie 2016 în ceea ce privește noul cadru pentru transferurile de date cu caracter personal, numit „Privacy Shield UE-SUA" (denumit în continuare Privacy Shield). La data de 29 februarie, Comisia Europeană a făcut public proiectul de decizie privind caracterul adecvat al acestui nou cadru (denumit în continuare proiectul de decizie) ([3]) și cele șapte anexe ale acestuia, inclusiv principiile Privacy Shield și declarațiile și angajamentele scrise ale oficialilor și autorităților SUA. AEPD a primi proiectul de decizie pentru consultare la data de 18 mai a acestui an.

AEPD și-a exprimat poziția în ceea ce privește transferurile de date cu caracter personal între UE și SUA într-o serie de ocazii ([4]) și a contribuit la Grupul de lucru „Articolul 29" (denumit în continuare GL29) Aviz privind proiectul de decizie, în calitate de membră a acestui grup ([5]). GL29 a prezentat motive de îngrijorare deosebită și a solicitat Comisiei Europene să identifice soluțiile în vederea adresării acestora. Membrii GL29 se așteaptă să primească toate clarificările necesare din aviz ([6]). La data de 16 martie, organizațiile non-profit au criticat proiectul de decizie într-o scrisoare adresată autorităților UE și SUA ([7]). La data de 26 mai, Parlamentul European a adoptat o rezoluție a fluxurilor de date transatlantice ([8]), care solicită Comisiei să negocieze alte îmbunătățiri ale aranjamentului Privacy Shield cu Administrația SUA, având în vedere deficiențele din prezent ([9]).

În calitate de consilier independent al legiuitorilor UE conform Regulamentului (CE) nr. 45/2001, AEPD emite acum recomandări părților implicate în proces, în special Comisiei. Această consiliere are scopul de a fi atât principială, cât și pragmatică, luând în considerare asistența proactivă acordată UE pentru îndeplinirea obiectivelor sale prin măsuri adecvate. Completează și subliniază unele recomandări, însă nu toate, ale Avizului GL29.

([1]) Cauza C-362/14, Maximillian Schrems împotriva Data Protection Commissioner, din 6 octombrie 2015 (denumită în continuare: „Schrems").

([2]) Decizia 2000/520/CE a Comisiei din 26 iulie 2000 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției oferite de principiile „sferei de siguranță" privind protecția vieții private și întrebările de bază aferente, publicate de Departamentul Comerțului al SUA [notificată cu numărul C(2000) 2441] (JO L 215, 25.8.2000, p. 7).

([3]) Decizia de punere în aplicare a Comisiei din XXX în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției oferite de Privacy-Shield UE-SUA, disponibilă la: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf

([4]) A se vedea Avizul Autorității Europene pentru Protecția Datelor privind Comunicarea Comisiei către Parlamentul European și Consiliu legată de „Restabilirea încrederii în fluxurile de date UE-SUA" și privind Comunicarea Comisiei către Parlamentul European și Consiliu referitoare la „funcționarea sferei de siguranță din perspectiva cetățenilor UE și a companiilor înființate în UE", de la data de 20 februarie 2014 și AEPD pledând la audierea CJUE din cauza Schrems, disponibile la: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2015/15-03-24_EDPS_Pleading_Schrems_vs_Data_Commissioner_EN.pdf).

([5]) Grupul de lucru „Articolul 29" în Avizul 01/2016 privind decizia adecvării Privacy Shield UE-SUA (GL 238) disponibil la http://ec.europa.eu/jus.tice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

([6]) A se vedea de asemenea discursul comisarului responsabil cu informațiile din Marea Britanie, Christopher Graham, din cadrul Conferinței IAPP Europa privind protecția intensivă a datelor cu caracter personal, susținută în Londra. Discursul (video) este disponibil și la: https://iapp.org/news/video/iapp-europe-data-protection-intensive-2016-christopher-graham-keynote/

([7]) Scrisoarea către Grupul de Lucru „Articolul 29" și celelalte instituții, semnată de Access Now și alte 26 de ONG-uri.

([8]) Decizia Parlamentului European din 26 mai 2016 privind fluxurile de date transatlantice [2016/2727(RSP)].

([9]) *Idem*, par. 14.

Proiectul de decizie prezintă o serie de îmbunătățiri prin comparație cu Decizia privind sfera de siguranță, în special în ceea ce privește principiile pentru procesarea datelor în scopuri comerciale. În ceea ce privește accesul autorităților publice la datele transferate conform Privacy Shield, salutăm de asemenea implicarea pentru prima dată în negocieri a Departamentului de Justiție, a Departamentului de Stat și Biroului Directorului Serviciilor Naționale de Informații. Însă nu este suficientă evoluția comparativă cu decizia anterioară privind sfera de siguranță. Criteriul corect de referință nu este o decizie anulată anterior, deoarece decizia privind caracterul adecvat nu se bazează pe cadrul legal UE în prezent (în special directiva în sine, articolul 16 din Tratatul privind funcționarea Uniunii Europene, precum și articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene, în forma interpretată de CJUE). Articolul 45 din Regulamentul general privind protecția datelor (denumit în continuare RPGD) ([1]) al UE va include cerințe noi pentru transferurile de date în baza unei decizii privind caracterul adecvat.

Anul trecut, CJUE a afirmat că pragul de evaluare a caracterului adecvat este „echivalența esențială” și a solicitat o evaluare strictă prin comparație cu acest standard ridicat ([2]). Caracterul adecvat nu necesită adoptarea unui cadru identic cu cel existent în UE, însă, luate ca întreg, Privacy Shield și ordinea juridică din SUA ar trebui să acopere toate elementele cheie ale cadrului UE de protecție a datelor. Acest lucru necesită atât o evaluare generală a ordinii juridice, cât și examinarea celor mai importante elemente ale cadrului UE de protecție a datelor ([3]). Presupunem că evaluarea ar trebui efectuată în termeni globali prin respectarea esenței acestor elemente. Mai mult, datorită tratatului și cartei, vor trebui luate în considerare elemente specifice cum ar fi supravegherea independentă și corectarea.

În această privință, AEPD cunoaște faptul că multe organizații de ambele părți ale Atlanticului așteaptă rezultatul acestei decizii privind caracterul adecvat. Însă consecințele unei noi anulări de către CJUE în termeni de incertitudine juridică pot fi mari pentru persoanele vizate, la fel ca povara suportată în special de IMM-uri. Mai mult, în cazul adoptării și anulării ulterioare a proiectului de decizie de către CJUE, toate aranjamentele noi privind caracterul adecvat vor trebui negociate conform RPGD. De aceea, recomandăm o abordare orientată către viitor, ținând cont de data iminentă a aplicării complete a RPGD peste doi ani.

Proiectul de decizie este cheia relațiilor dintre UE și SUA, într-un moment în care fac inclusiv subiectul negocierilor comerciale și de investiții. Mai mult, multe dintre elementele luate în considerare în avizul nostru sunt relevante indirect atât pentru Privacy Shield și alte instrumente de transfer, cum ar fi Regulile Corporatiste Obligatorii (denumite în continuare RCO) și Clauzele Contractuale Standard (denumite în continuare CCS). Acesta are de asemenea și o relevanță globală, deoarece multe țări terțe îl vor urmări îndeaproape pe fondul adoptării noului cadru UE privind protecția datelor.

De aceea, am saluta o soluție generală pentru transferurile UE-SUA, cu condiția ca aceasta să fie cuprinzătoare și suficient de solidă. Acest lucru necesită îmbunătățiri robuste, pentru a asigura respectarea sustenabilă pe termen lung a drepturilor și a libertăților noastre fundamentale. În cazul adoptării, la prima evaluare de către Comisia Europeană, decizia trebuie să fie revizuită la timp, pentru a identifica etapele relevante pentru soluțiile pentru termen mai lung, pentru înlocuirea Privacy Shield cu un cadru legal mai robust și mai stabil pentru amplificarea relațiilor transatlantice.

AEPD menționează de asemenea din proiectul de decizie și anexele sale că, neținând seama de tendințele recente de a trece de la supravegherea fără discriminare pe bază generală către abordări mai țintite și selectate, scara sistemului de colectare a informațiilor și volumul de date transferat din UE, făcând subiectul posibilei colectări odată transferate și în mod notabil în timpul tranzitului, poate fi încă ridicată, putând fi pusă sub semnul întrebării.

Deși aceste practici pot fi de asemenea legate de serviciile de informații din alte țări și chiar dacă salutăm transparența autorităților SUA în ceea ce privește această nouă realitate, proiectul de decizie din prezent poate fi interpretat ca oferind legitimitate acestei rutine. Această problemă necesită un control public democratic serios. De aceea, încurajăm Comisia Europeană să transmită un semnal mai puternic: date fiind obligațiile ce îi revin UE conform Tratatului de la Lisabona, accesul și folosirea de către autoritățile publice a datelor transferate în scopuri comerciale, inclusiv în tranzit, ar trebui să aibă loc ca excepție și acolo unde acest lucru este indispensabil pentru scopurile specificate de interes public.

Mai mult, observăm că declarațiile esențiale relevante pentru viețile private ale persoanelor fizice în UE par a fi elaborate numai detaliile importante în scrisorile interne către autoritățile SUA (de exemplu, declarațiile referitoare la activitățile de

([1]) Regulamentul (UE) 2016/679 al Parlamentului European și Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește procesarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

([2]) Schrems, par. 71, 73, 74 și 96.

([3]) Această abordare a fost deja luată în considerare într-una din lucrările anterioare ale GL29 referitoare la transferurile de date (GL12: „Document de lucru privind transferul de date cu caracter personal către țări terțe: Punerea în aplicare a articolelor 25 și 26 din Directiva UE privind protecția datelor”, 24 iulie 1998).

colectare a informațiilor prin cabluri transatlantice, dacă este cazul) ([1]). Deși nu punem la îndoială autoritatea distinșilor lor autori și înțelegem că, odată publicate în Jurnalul Oficial și Registrul Federal, aceste declarații vor fi considerate ca fiind „asigurări în scris" în baza cărora se face evaluarea UE, menționăm în general că importanța unora dintre aceste declarații ar merita o valoare juridică mai mare.

Pe lângă modificarea legislativă și acordurile internaționale ([2]), se pot explora și soluții practice suplimentare. Avizul nostru are drept scop oferirea unor sfaturi pragmatice în această privință.

IV. **Concluzie**

AEPD salută eforturile făcute de părți pentru identificarea unei soluții de transfer al datelor cu caracter personal din UE către SUA, în scopuri comerciale, în cadrul unui sistem de declarații de conformitate. Însă sunt necesare îmbunătățiri mai robuste, pentru a realiza un cadru solid, stabil pe termen lung.

Încheiată în Bruxelles, 30 mai 2016.

Giovanni BUTTARELLI

Autoritatea Europeană pentru Protecția Datelor

([1]) A se vedea de exemplu clarificările din Anexa VI.1 litera (a), care ar fi aplicate de PPD28 datelor colectate prin cablurile transatlantice de către Comunitatea de Informații SUA.

([2]) La audierea CJUE în cauza Schrems, AEPD a declarat că „Singura soluție eficientă este negocierea unui acord internațional care să prevadă protecția adecvată contra supravegherii fără discriminare, inclusiv obligații privind supravegherea, transparența, corecția și drepturile privind protecția datelor cu caracter personal", în pledoaria din cadru audierii Curții de Justiție din 24 martie 2015 în cauza C-362/14 (Schrems împotriva Data Protection Commissioner).