Recomandări

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Recomandările 01/2020 privind măsurile care completează instrumentele de transfer pentru a asigura conformitatea cu nivelul UE de protecție a datelor cu caracter personal

Adoptate la 10 noiembrie 2020

Rezumat

Regulamentul general al UE privind protecția datelor (RGPD) a fost adoptat pentru a răspunde unei duble finalități: facilitarea liberei circulații a datelor cu caracter personal în cadrul Uniunii Europene și protejarea drepturilor și libertăților fundamentale ale persoanelor, în special dreptul acestora la protecția datelor cu caracter personal.

În hotărârea sa recentă C-311/18 (Schrems II), Curtea de Justiție a Uniunii Europene (CJUE) ne reamintește că protecția acordată datelor cu caracter personal în Spațiul Economic European (SEE) trebuie să însoțească datele oriunde s-ar afla acestea. Transferul de date cu caracter personal către țări terțe nu poate fi un mijloc de subminare sau de reducere a protecției de care beneficiază în SEE. De asemenea, Curtea clarifică acest aspect afirmând că nivelul de protecție în țările terțe nu trebuie să fie identic cu cel garantat în SEE, ci, în esență, echivalent. Curtea susține, de asemenea, validitatea clauzelor contractuale standard, ca instrument de transfer care poate servi la asigurarea prin contract a unui nivel de protecție în esență echivalent în cazul datelor transferate către țări terțe.

Clauzele contractuale standard și alte instrumente de transfer menționate la articolul 46 din RGPD sunt inoperante în situații de vid juridic. Curtea afirmă că operatorii sau persoanele împuternicite de operatori, care acționează în calitate de exportatori, au responsabilitatea de a verifica, de la caz la caz și, dacă este necesar, în colaborare cu importatorul din țara terță, dacă legislația sau practica țării terțe aduce atingere eficacității garanțiilor adecvate cuprinse în instrumentele de transfer prevăzute la articolul 46 din RGPD. În aceste cauze, Curtea lasă totuși deschisă posibilitatea ca exportatorii să pună în aplicare măsuri suplimentare care să acopere aceste lacune în ceea ce privește protecția și să o aducă la nivelul impus de dreptul Uniunii. Curtea nu precizează care ar putea fi aceste măsuri. Totuși, Curtea subliniază că exportatorii vor trebui să le identifice de la caz la caz. Aceasta este în conformitate cu principiul responsabilității prevăzut la articolul 5 alineatul (2) din RGPD, care impune operatorilor să fie responsabili și să poată demonstra conformitatea cu principiile RGPD referitoare la prelucrarea datelor cu caracter personal.

Pentru a-i ajuta pe exportatori (indiferent dacă sunt operatori sau persoane împuternicite de operatori, entități private sau organisme publice, care prelucrează date cu caracter personal ce se încadrează în domeniul de aplicare al RGPD) să-și îndeplinească sarcina complexă de a evalua țările terțe și de a identifica măsuri suplimentare adecvate acolo unde este necesar, Comitetul european pentru protecția datelor (CEPD) adoptă prezentele recomandări. Prezentele recomandări oferă exportatorilor o serie de pași de urmat, surse potențiale de informații și câteva exemple de măsuri suplimentare care ar putea fi puse în aplicare.

Ca un **prim pas**, CEPD vă recomandă dumneavoastră, exportatorilor, să **cunoașteți detaliile transferurilor**. Cartografierea tuturor transferurilor de date cu caracter personal către țări terțe poate fi un exercițiu dificil. Este totuși necesar să știți unde se află datele cu caracter personal pentru a vă asigura că acestea beneficiază de un nivel de protecție în esență echivalent, indiferent de locul în care sunt prelucrate. De asemenea, trebuie să verificați dacă datele pe care le transferați sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt transferate și prelucrate în țara terță.

Un **al doilea** pas constă în **verificarea instrumentului de transfer pe care se bazează transferul**, dintre cele enumerate în capitolul V din RGPD. În cazul în care Comisia Europeană a declarat deja drept adecvată țara, regiunea sau sectorul în care transferați datele, prin intermediul uneia dintre deciziile sale privind caracterul adecvat al nivelului de protecție în temeiul articolului 45 din RGPD sau al Directivei 95/46 anterioare, atât timp cât decizia este încă în vigoare, nu va trebui să luați alte măsuri

decât să monitorizați că decizia privind caracterul adecvat rămâne valabilă. În absența unei decizii privind caracterul adecvat al nivelului de protecție, trebuie să vă bazați pe unul dintre instrumentele de transfer enumerate la articolul 46 din RGPD în cazul transferurilor regulate și repetate. Numai în unele cazuri de transferuri ocazionale și nerepetitive vă puteți prevala de una dintre derogările prevăzute la articolul 49 din RGPD, dacă îndepliniți condițiile.

Un **al treilea** pas constă în **evaluarea** existenței în **legislația sau în practica țării terțe** a vreunui element care ar putea aduce atingere eficacității garanțiilor adecvate ale instrumentelor de transfer pe care vă bazați, în contextul transferului dumneavoastră specific. Evaluarea dumneavoastră ar trebui să vizeze, în primul rând, legislația țării terțe care este relevantă pentru transferul dumneavoastră și instrumentul de transfer prevăzut la articolul 46 din RGPD pe care vă bazați și care ar putea submina nivelul de protecție al acestuia. Pentru evaluarea elementelor care trebuie luate în considerare la evaluarea legislației unei țări terțe care abordează accesul autorităților publice la date în scopul supravegherii, vă rugăm să consultați recomandările CEPD privind garanțiile esențiale europene. În special, acest lucru ar trebui analizat cu atenție atunci când legislația care reglementează accesul autorităților publice la date este ambiguă sau nu este disponibilă publicului. În lipsa unei legislații care să reglementeze împrejurările în care autoritățile publice pot avea acces la date cu caracter personal, dacă încă mai doriți să efectuați transferul, ar trebui să analizați alți factori relevanți și obiectivi și să nu vă bazați pe factori subiectivi, cum ar fi probabilitatea ca autoritățile publice să aibă acces la datele dumneavoastră într-un mod care contravine standardelor UE. Ar trebui să efectuați această evaluare cu diligența necesară și să o documentați temeinic, întrucât veți fi tras la răspundere pentru decizia pe care o puteți lua în consecință.

Un **al patrulea pas** constă în **identificarea și adoptarea măsurilor suplimentare** necesare pentru a aduce nivelul de protecție a datelor transferate la standardul UE de echivalență esențială. Acest pas este necesar numai dacă evaluarea dumneavoastră arată că legislația țării terțe aduce atingere eficacității instrumentului de transfer prevăzut la articolul 46 din RGPD pe care vă bazați sau intenționați să vă bazați în contextul transferului dumneavoastră. Prezentele recomandări conțin (în anexa 2) o listă neexhaustivă de exemple de măsuri suplimentare însoțite de unele condiții necesare pentru ca acestea să fie eficace. La fel ca în cazul garanțiilor adecvate cuprinse în instrumentele de transfer prevăzute la articolul 46, unele măsuri suplimentare pot fi eficace în unele țări, dar nu neapărat și în altele. Veți fi responsabil pentru evaluarea eficacității acestora în contextul transferului și în raport cu legislația țării terțe și cu instrumentul de transfer pe care vă bazați și veți fi tras la răspundere pentru decizia pe care o luați. În acest scop ar putea fi, de asemenea, necesar să combinați mai multe măsuri suplimentare. La final, este posibil să constatați că nicio măsură suplimentară nu poate asigura un nivel de protecție în esență echivalent pentru transferul dumneavoastră specific. În cazurile în care nu este adecvată nicio măsură suplimentară, trebuie să evitați, să suspendați sau să încetați transferul, pentru a nu compromite nivelul de protecție a datelor cu caracter personal. De asemenea, ar trebui să efectuați această evaluare a măsurilor suplimentare cu diligența necesară și să o documentați.

Un **al cincea pas** constă în **inițierea** oricăror **formalități procedurale** pe care le poate impune adoptarea măsurii dumneavoastră suplimentare, în funcție de instrumentul de transfer prevăzut la articolul 46 din RGPD pe care vă bazați. Prezentele recomandări precizează aceste formalități. Este posibil să fie necesară consultarea autorităților de supraveghere competente cu privire la unele dintre acestea.

Al șaselea pas și ultimul va consta în reevaluarea, la intervale corespunzătoare, a nivelului de protecție de care beneficiază datele pe care le transferați către țări terțe și monitorizarea existenței anterioare sau viitoare a unor evoluții care l-ar putea afecta. Principiul responsabilității necesită o monitorizare continuă a nivelului de protecție a datelor cu caracter personal.

Autoritățile de supraveghere vor continua să își exercite mandatul privind monitorizarea aplicării RGPD și asigurarea respectării acestuia. Autoritățile de supraveghere vor acorda atenția cuvenită măsurilor pe care exportatorii le iau pentru a se asigura că datele pe care le transferă beneficiază de un nivel de protecție în esență echivalent. Astfel cum amintește Curtea, autoritățile de supraveghere vor suspenda sau vor interzice transferurile de date în cazurile în care, în urma unei anchete sau a unei plângeri, constată că nu poate fi asigurat un nivel de protecție în esență echivalent.

Autoritățile de supraveghere vor continua să elaboreze ghiduri pentru exportatori și să-și coordoneze acțiunile în cadrul CEPD pentru a asigura punerea în aplicare consecventă a legislației UE privind protecția datelor.

Cuprins

Comitetul european pentru protecția datelor,

având în vedere articolul 70 alineatul (1) litera (e) din Regulamentul 2016/679/UE al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (denumit în continuare „RGPD"),

având în vedere Acordul privind Spațiul Economic European (SEE), în special anexa XI și Protocolul 37 la acesta, astfel cum au fost modificate prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018[1],

având în vedere articolele 12 și 22 din Regulamentul său de procedură,

întrucât:

(1) Curtea de Justiție a Uniunii Europene (CJUE) concluzionează în hotărârea sa din 16 iulie 2020, *Data Protection Commissioner/Facebook Ireland LTD, Maximillian Schrems,* C-311/18, că articolul 46 alineatul (1) și articolul 46 alineatul (2) litera (c) din RGPD trebuie interpretate în sensul că garanțiile adecvate, drepturile opozabile și căile de atac eficiente prevăzute de aceste dispoziții trebuie să asigure că drepturile persoanelor ale căror date cu caracter personal sunt transferate către o țară terță în temeiul unor clauze standard de protecție a datelor beneficiază de un nivel de protecție în esență echivalent cu cel garantat în Uniunea Europeană de regulamentul menționat, interpretat în lumina Cartei drepturilor fundamentale a Uniunii Europene[2].

(2) Astfel cum a subliniat Curtea, trebuie garantat un nivel de protecție a persoanelor fizice în esență echivalent cu cel garantat în cadrul Uniunii Europene prin RGPD, interpretat în lumina cartei, indiferent de dispoziția din capitolul V pe baza căreia se efectuează un transfer de date cu caracter personal către o țară terță. Dispozițiile din capitolul V urmăresc să asigure continuitatea acestui nivel ridicat de protecție în cazul în care datele cu caracter personal sunt transferate către o țară terță[3].

(3) Considerentul 108 și articolul 46 alineatul (1) din RGPD prevăd că în absența unei decizii a UE privind caracterul adecvat al nivelului de protecție, operatorul sau persoana împuternicită de operator trebuie să adopte măsuri pentru a compensa lipsa protecției datelor într-o țară terță prin intermediul unor garanții adecvate pentru persoana vizată. Un operator sau o persoană împuternicită de operator poate oferi garanții adecvate, fără să fie nevoie de nicio autorizație specifică din partea unei autorități de supraveghere, utilizând unul dintre instrumentele de transfer enumerate la articolul 46 alineatul (2) din RGPD, cum ar fi clauzele standard de protecție a datelor.

[1] Referirile la „statele membre" din acest document trebuie înțelese ca referiri la „statele membre ale SEE".
[2] Hotărârea CJUE din 16 iulie 2020, *Data Protection Commissioner/Facebook Ireland Ltd, Maximillian Schrems, [denumită în continuare* C-311/18 (Schrems II)], a doua constatare.
[3] C-311/18 (Schrems II), punctele 92 și 93.

(4) Curtea clarifică faptul că clauzele standard de protecție a datelor adoptate de Comisie nu urmăresc decât să ofere operatorilor și persoanelor împuternicite de operatori stabilite în Uniunea Europeană garanții contractuale care să se aplice în mod uniform în toate țările terțe. Având în vedere caracterul lor contractual, clauzele standard de protecție a datelor nu pot fi obligatorii pentru autoritățile publice ale țărilor terțe, deoarece acestea nu sunt părți la contract. În consecință, ar putea fi necesar ca exportatorii de date să completeze garanțiile cuprinse în aceste clauze standard de protecție a datelor cu măsuri suplimentare, pentru a asigura respectarea nivelului de protecție impus de dreptul Uniunii într-o anumită țară terță. Curtea face trimitere la considerentul 109 din RGPD, care menționează această posibilitate și încurajează operatorii și persoanele împuternicite de operatori să o utilizeze[4].

(5) Curtea a precizat că revine în primul rând exportatorului de date sarcina de a verifica, de la caz la caz și, dacă este necesar, în colaborare cu importatorul de date, dacă dreptul țării terțe de destinație asigură un nivel de protecție în esență echivalent, din perspectiva dreptului Uniunii, al datelor cu caracter personal transferate în temeiul unor clauze standard de protecție a datelor, la nevoie prin asigurarea unor măsuri suplimentare față de cele oferite de clauzele menționate[5].

(6) Dacă operatorul sau o persoană împuternicită de operator stabilită în Uniunea Europeană nu poate lua măsuri suplimentare adecvate pentru a garanta un nivel de protecție în esență echivalent, din perspectiva dreptului UE, aceasta sau, în subsidiar, autoritatea de supraveghere competentă, este obligată să suspende sau să înceteze transferul de date cu caracter personal către țara terță în cauză[6].

(7) RGPD sau Curtea nu definește sau nu specifică „garanțiile suplimentare”, „măsurile suplimentare” sau „măsurile suplimentare” garanțiilor instrumentelor de transfer enumerate la articolul 46 alineatul (2) din RGPD pe care operatorii și persoanele împuternicite de operatori le pot adopta pentru a asigura respectarea nivelului de protecție impus de dreptul Uniunii într-o anumită țară terță.

(8) CEPD a decis, din proprie inițiativă, să examineze această chestiune și să ofere operatorilor și persoanelor împuternicite de operatori, care acționează în calitate de exportatori, recomandări cu privire la procesul pe care îl pot urma pentru a identifica și a adopta măsuri suplimentare. Prezentele recomandări urmăresc să ofere exportatorilor o metodologie pentru a stabili dacă ar trebui puse în aplicare măsuri suplimentare pentru transferurile lor și care ar trebui să fie acestea. Este responsabilitatea principală a exportatorilor să se asigure că datele transferate beneficiază în țara terță de un nivel de protecție în esență echivalent cu cel garantat în UE. Prin prezentele recomandări, CEPD urmărește să încurajeze aplicarea consecventă a RGPD și a hotărârii Curții, în temeiul mandatului CEPD[7]

ADOPTĂ URMĂTOAREA RECOMANDARE:

[4] C-311/18 (Schrems II), punctele 132 și 133.
[5] C-311/18 (Schrems II), punctul 134.
[6] C-311/18 (Schrems II), punctul 135.
[7] Articolul 70 alineatul (1) litera (e) din RGPD.

1 RESPONSABILITATEA ÎN CEEA CE PRIVEȘTE TRANSFERURILE DE DATE

1. Dreptul primar al UE consideră că dreptul la protecția datelor este un drept fundamental[8]. În consecință, dreptul la protecția datelor beneficiază de un nivel ridicat de protecție și pot fi impuse restrângeri ale acestuia numai dacă sunt prevăzute de lege, respectă substanța acestui drept, sunt proporționale, necesare și răspund efectiv unor obiective de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți[9]. Dreptul la protecția datelor cu caracter personal nu este un drept absolut; acesta trebuie luat în considerare în raport cu funcția pe care o îndeplinește în societate și echilibrat cu alte drepturi fundamentale, în conformitate cu principiul proporționalității[10].

2. Un nivel de protecție în esență echivalent cu cel garantat în UE trebuie să însoțească datele când sunt transferate către țări terțe din afara SEE pentru a se asigura că nivelul de protecție garantat de RGPD nu este subminat.

3. Dreptul la protecția datelor are un caracter activ. Aceasta impune exportatorilor și importatorilor (indiferent dacă sunt operatori și/sau persoane împuternicite de operatori) să meargă dincolo de o recunoaștere sau o respectare pasivă a acestui drept[11]. Operatorii și persoanele împuternicite de operatori trebuie să încerce să respecte dreptul la protecția datelor în mod activ și continuu prin punerea în aplicare a unor măsuri juridice, tehnice și organizatorice care să-i asigure eficacitatea. Operatorii și persoanele împuternicite de operatori trebuie, de asemenea, să poată demonstra aceste eforturi persoanelor vizate, publicului larg și autorităților de supraveghere a protecției datelor. Acesta este așa-numitul principiu al responsabilității[12].

4. Principiul responsabilității, care este necesar pentru a asigura aplicarea efectivă a nivelului de protecție conferit prin RGPD, se aplică, de asemenea, transferurilor de date către țări terțe[13], deoarece acestea constituie, în sine, o formă de prelucrare a datelor[14]. Astfel cum a subliniat Curtea în hotărârea sa, trebuie garantat un nivel de protecție în esență echivalent cu cel garantat în cadrul Uniunii Europene prin RGPD, interpretat în lumina cartei, indiferent de dispoziția din capitolul respectiv pe baza căreia se efectuează un transfer de date cu caracter personal către o țară terță[15].

5. În hotărârea Schrems II, Curtea subliniază responsabilitățile exportatorilor și importatorilor de a se asigura că prelucrarea datelor cu caracter personal a fost și va continua să fie efectuată în conformitate cu nivelul de protecție stabilit de legislația UE privind protecția datelor și de a suspenda transferul și/sau de a rezilia contractul în cazul în care importatorul de date nu este sau nu mai este în măsură să respecte clauzele standard de protecție a datelor incluse în contractul relevant dintre exportator și importator[16]. Operatorul sau persoana împuternicită de operator care acționează în calitate de

[8] Articolul 8 alineatul (1) din Carta drepturilor fundamentale și articolul 16 alineatul (1) din TFUE, preambulul 1, articolul 1 alineatul (2) din RGPD.
[9] Articolul 52 alineatul (1) din Carta drepturilor fundamentale a UE.
[10] Considerentul 4 din RGPD și cauza C-507/17 Google LLC, succesoare în drepturi a Google Inc./Commission nationale de l'informatique et des libertés (CNIL), punctul 60.
[11] Vezi C□92/09 și C□93/02, Volker und Markus Schecke GbR/Land Hessen, Concluziile avocatului general E. Sharpston, 17 iunie 2010, punctul 71.
[12] Articolul 5 alineatul (2) și articolul 28 alineatul (3) litera (h) din RGPD.
[13] Articolul 44 și considerentul 101 din RGPD, precum și articolul 47 alineatul (2) litera (d) din RGPD.
[14] Hotărârea CJUE din 6 octombrie 2015, *Maximillian Schrems/Data Protection Commissioner [denumită în continuare* C-362/14 (Schrems I)], punctul 45.
[15] C-311/18 (Schrems II), punctele 92 și 93.
[16] C-311/18 (Schrems II), punctele 134, 135, 139, 140, 141, 142.

exportator trebuie să se asigure că importatorii colaborează cu exportatorul, dacă este necesar, în îndeplinirea acestor responsabilități, informându-l, de exemplu, cu privire la evoluțiile care afectează nivelul de protecție a datelor cu caracter personal primite în țara importatorului[17]. Aceste responsabilități reprezintă o aplicare a principiului responsabilității din RGPD în cazul transferurilor de date.[18].

2 FOAIE DE PARCURS: APLICAREA EFECTIVĂ A PRINCIPIULUI RESPONSABILITĂȚII ÎN CAZUL TRANSFERURILOR DE DATE

6. Urmează o foaie de parcurs a măsurilor care trebuie luate pentru a afla dacă dumneavoastră (exportatorul de date) trebuie să puneți în aplicare măsuri suplimentare pentru a putea transfera în mod legal date în afara SEE. În prezentul document, „dumneavoastră" înseamnă operatorul sau persoana împuternicită de operator care acționează în calitate de exportator de date, care prelucrează date cu caracter personal ce se încadrează în domeniul de aplicare al RGPD – inclusiv entități private și organisme publice atunci când se transferă date către organisme private[19]. În ceea ce privește transferurile de date cu caracter personal efectuate între organisme publice, sunt prevăzute indicații specifice în *Orientările nr. 2/2020 referitoare la articolul 46 alineatul (2) litera (a) și articolul 46 alineatul (3) litera (b) din Regulamentul (UE) 2016/679 pentru transferuri de date cu caracter personal între autorități și organisme publice din SEE și din afara SEE.*[20]

7. Va fi necesar să documentați în mod corespunzător această evaluare și măsurile suplimentare selectate și să le puneți la dispoziția autorității de supraveghere competente, la cerere[21].

2.1 Pasul 1: Cunoașterea detaliilor transferurilor

8. Pentru a ști care ar putea fi cerințele pentru dumneavoastră (exportatorul de date) pentru a putea continua sau efectua noi transferuri de date cu caracter personal[22], primul pas este să vă asigurați că sunteți pe deplin informat cu privire la transferurile dumneavoastră (cunoașteți detaliile transferurilor). Înregistrarea și cartografierea tuturor transferurilor pot fi un exercițiu complex pentru entitățile care efectuează transferuri multiple, diverse și regulate cu țări terțe și care utilizează o serie de persoane împuternicite de operator și subcontractanți. Cunoașterea detaliilor transferurilor este un prim pas esențial în îndeplinirea obligațiilor care vă revin în temeiul principiului responsabilității.

[17] C-311/18 (Schrems II), punctul 134.
[18] Articolul 5 alineatul (2) și articolul 28 alineatul (3) litera (h) din RGPD.
[19] CEPD, Orientările nr. 3/2018 privind domeniul de aplicare teritorial al RGPD (articolul 3) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_ro
[20] CEPD, Orientările nr. 2/2020 referitoare la articolul 46 alineatul (2) litera (a) și articolul 46 alineatul (3) litera (b) din Regulamentul (UE) 2016/679 pentru transferuri de date cu caracter personal între autorități și organisme publice din SEE și din afara SEE; vezi https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_ro
[21] Articolul 5 alineatul (2) din RGPD și articolul 24 alineatul (1) din RGPD.
[22] Vă atragem atenția că accesarea de la distanță de către o entitate dintr-o țară terță a datelor stocate în SEE este, de asemenea, considerată transfer.

9. Pentru a fi pe deplin informat cu privire la transferurile dumneavoastră, vă puteți baza pe evidențele activităților de prelucrare pe care ați putea fi obligat să le păstrați în calitate de operator sau de persoană împuternicită de operator în temeiul articolului 30 din RGPD[23]. De asemenea, vă pot ajuta și acțiunile anterioare de îndeplinire a obligațiilor de informare a persoanelor vizate în temeiul articolelor 13 alineatul (1) litera (f) și 14 alineatul (1) litera (f) din RGDP cu privire la transferurile dumneavoastră de date cu caracter personal către țări terțe[24].

10. Când cartografiați transferurile, nu uitați să luați în considerare și transferurile ulterioare, de exemplu dacă persoanele din afara SEE împuternicite de operator transferă unui subcontractant dintr-o altă țară terță sau din aceeași țară terță datele cu caracter personal încredințate acestora[25].

11. În conformitate cu principiul „reducerii la minimum a datelor" din RPGD,[26] trebuie să verificați dacă datele pe care le transferați sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt transferate și prelucrate în țara terță.

12. Aceste activități trebuie să se realizeze înainte ca transferurile să fie efectuate și actualizate anterior reluării acestora după suspendarea operațiunilor de transfer de date: trebuie să știți unde pot fi stocate sau prelucrate de către importatori (harta destinațiilor) datele cu caracter personal pe care le-ați exportat.

13. Rețineți că accesul de la distanță dintr-o țară terță (de exemplu, în situații de acordare de asistență) și/sau stocarea într-un cloud situat în afara SEE sunt considerate, de asemenea, transfer[27]. Mai precis, dacă utilizați o infrastructură internațională de tip cloud, trebuie să evaluați dacă datele dumneavoastră vor fi transferate către țări terțe și unde, cu excepția cazului în care furnizorul de cloud precizează clar în contractul său că datele nu vor fi prelucrate deloc în țări terțe.

[23] Vezi articolul 30 din RGDP, în special alineatul (1) litera (e) și alineatul (2) litera (c). În plus, evidențele activităților dumneavoastră de prelucrare ar trebui să conțină o descriere a acestora (inclusiv, dar nu fără a se limita la categoriile de persoane vizate, categoriile de date cu caracter personal și scopurile prelucrării și informații specifice cu privire la transferurile de date. Unii operatori și unele persoane împuternicite de operatori sunt scutite de obligația de a păstra o evidență a activităților de prelucrare [articolul 30 alineatul (5) din RGPD]. Pentru îndrumări cu privire la această excepție, vezi documentul de poziție al Grupului de lucru „Articolul 29" privind derogările de la obligația de a păstra evidențe ale activităților de prelucrare în temeiul articolului 30 alineatul (5) din RGPD (aprobat de CEPD la 25 mai 2018).

[24] Conform normelor de transparență din RGPD, trebuie să informați persoanele vizate cu privire la transferurile de date cu caracter personal către țări terțe [articolul 13 alineatul (1) litera (f) și articolul 14 alineatul (1) litera (f) din RGPD]. În special, trebuie să le informați cu privire la existența sau absența unei decizii a Comisiei Europene privind caracterul adecvat al nivelului de protecție sau, în cazul transferurilor menționate la articolul 46 sau 47 din RGPD sau la articolul 49 alineatul (1) al doilea paragraf din RGPD, să faceți trimitere la garanțiile adecvate sau corespunzătoare și la mijloacele de a obține o copie a acestora, în cazul în care acestea au fost puse la dispoziție. Informațiile furnizate persoanei vizate trebuie să fie corecte și actuale, în special în lumina jurisprudenței Curții privind transferurile.

[25] În cazul în care operatorul a acordat în prealabil autorizația scrisă, specifică sau generală, în conformitate cu articolul 28 alineatul (2) din RGPD.

[26] Articolul 5 alineatul (1) litera (c) din RGPD.

[27] Vezi întrebarea frecventă nr. 11 „*trebuie avut în vedere că chiar și furnizarea accesului la date dintr-o țară terță, de exemplu în scopuri de administrare, reprezintă un transfer*", Întrebări frecvente cu privire la hotărârea Curții de Justiție a Uniunii Europene în cauza C-311/18 – Data Protection Commissioner împotriva Facebook Ireland Ltd și Maximillian Schrems, adoptate de CEPD la 23 iulie 2020.

2.2 Pasul 2: Identificarea instrumentelor de transfer pe care vă bazați

14. Al doilea pas pe care trebuie să îl faceți este să identificați instrumentele de transfer pe care vă bazați printre cele enumerate și avute în vedere la capitolul V din RGPD.

Decizii privind caracterul adecvat al nivelului de protecție

15. Comisia Europeană poate recunoaște, prin intermediul **deciziilor sale privind caracterul adecvat al nivelului de protecție** referitoare la unele sau toate țările terțe către care transferați date cu caracter personal, că acestea oferă un nivel adecvat de protecție a datelor cu caracter personal[28].

16. Efectul unei astfel de decizii privind caracterul adecvat al nivelului de protecție este că datele cu caracter personal pot circula din SEE către țara terță în cauză, fără a mai fi necesare alte instrumente de transfer în temeiul articolului 46 din RGPD.

17. Deciziile privind caracterul adecvat al nivelului de protecție se pot aplica la nivelul unei țări în ansamblu sau se pot limita la o parte a acesteia. Deciziile privind caracterul adecvat al nivelului de protecție se pot aplica tuturor transferurilor de date către o țară sau pot fi limitate la anumite tipuri de transferuri (de exemplu, într-un singur sector)[29].

18. Comisia Europeană publică pe site-ul său lista deciziilor sale privind caracterul adecvat al nivelului de protecție[30].

19. Dacă transferați date cu caracter personal către țări terțe, regiuni sau sectoare care fac obiectul unei decizii a Comisiei privind caracterul adecvat al nivelului de protecție (în măsura aplicabilă), **nu este necesar să luați alte măsuri, astfel cum se descrie în prezentele recomandări.**[31] Cu toate acestea, trebuie să monitorizați în continuare dacă deciziile privind caracterul adecvat al nivelului de protecție relevante pentru transferurile dumneavoastră sunt revocate sau invalidate[32].

[28] Comisia Europeană are competența de a stabili, în temeiul articolului 45 din RGPD, dacă o țară din afara UE oferă un nivel adecvat de protecție a datelor. De asemenea, Comisia Europeană are competența de a stabili dacă o organizație internațională oferă un nivel adecvat de protecție.

[29] Articolul 45 alineatul (1) din RGPD.

[30] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_ro

[31] Cu condiția ca dumneavoastră și importatorul de date să fi pus în aplicare măsuri pentru respectarea celorlalte obligații prevăzute în RGPD; în caz contrar, puneți în aplicare măsurile respective.

[32] Comisia Europeană trebuie să revizuiască periodic toate deciziile privind caracterul adecvat al nivelului de protecție și să monitorizeze dacă țările terțe care beneficiază de decizii privind caracterul adecvat al nivelului de protecție continuă să asigure un nivel adecvat de protecție [vezi articolul 45 alineatul (3) și articolul 45 alineatul (4) din RGPD]. De asemenea, CJUE poate anula deciziile privind caracterul adecvat al nivelului de protecție [vezi hotărârile sale în cauzele C-362/14 (Schrems I) și C-311/18 (Schrems II)].

20. Cu toate acestea, deciziile privind caracterul adecvat al nivelului de protecție nu împiedică persoanele vizate să depună plângeri. Acestea nici nu împiedică autoritățile de supraveghere să sesizeze o instanță națională dacă au îndoieli cu privire la validitatea unei decizii, pentru ca instanța națională să poată adresa CJUE o cerere de pronunțare a unei hotărâri preliminare în vederea examinării validității[33].

Exemplu: În iunie 2013, un cetățean al UE, dl Schrems, a depus o plângere la Comisia pentru protecția datelor (Data Protection Commission - DPC) din Irlanda solicitând acestei autorități de supraveghere să interzică sau să suspende transferul datelor sale cu caracter personal de la Facebook Ireland către Statele Unite, considerând că legislația și practicile Statelor Unite nu asigurau o protecție adecvată a datelor cu caracter personal stocate pe teritoriul său împotriva activităților de supraveghere practicate de autoritățile publice în această țară. DPC a respins plângerea, în special pentru motivul că, în Decizia 2000/520, Comisia Europeană a considerat că, în cadrul sistemului „sferei de siguranță", Statele Unite asigură un nivel adecvat de protecție a datelor cu caracter personal transferate („Decizia privind sfera de siguranță"). Dl Schrems a contestat decizia DPC, iar High Court (Înalta Curte) din Irlanda a adresat Curții de Justiție a Uniunii Europene (CJUE) o întrebare privind validitatea Deciziei 2000/520. CJUE a decis ulterior să invalideze Decizia 2000/520 a Comisiei privind caracterul adecvat al protecției oferite de principiile „sferei de siguranță" privind protecția vieții private[34].

Instrumentele de transfer de la articolul 46 din RGPD

21. Articolul 46 din RGPD enumeră o serie de instrumente de transfer care conțin *„garanțiile adecvate"* pe care exportatorii le pot utiliza pentru a transfera date cu caracter personal către țări terțe în absența unor decizii privind caracterul adecvat al nivelului de protecție. Principalele tipuri de instrumente de transfer prevăzute la articolul 46 din RGPD sunt:

- clauze standard de protecție a datelor (CCS);
- reguli corporatiste obligatorii (BCR);
- coduri de conduită;
- mecanisme de certificare;
- clauze contractuale ad-hoc.

22. Indiferent de instrumentul de transfer prevăzut la articolul 46 din RGPD pe care îl alegeți, trebuie să vă asigurați că, în ansamblu, datele cu caracter personal transferate vor beneficia de un nivel de protecție în esență echivalent.

23. Instrumentele de transfer prevăzute la articolul 46 din RGPD conțin, în principal, garanții adecvate de natură contractuală care pot fi aplicate transferurilor către toate țările terțe. Situația din țara terță în care transferați datele poate impune totuși completarea acestor instrumente de transfer și a

[33] C-311/18 (Schrems II), punctele 118-120. Autoritățile de supraveghere nu pot să ignore decizia privind caracterul adecvat al nivelului de protecție și să suspende sau să interzică transferurile de date cu caracter personal către astfel de țări, invocând doar caracterul inadecvat al nivelului de protecție. Acestea își pot exercita competența de a suspenda sau de a interzice transferurile de date cu caracter personal către țara terță respectivă numai din alte motive (de exemplu, măsuri de securitate insuficiente care încalcă articolul 32 din RGPD, lipsa unui temei juridic care să justifice prelucrarea datelor ca atare, cu încălcarea articolului 6 din RGPD). Autoritățile de supraveghere pot examina, în condiții de independență deplină, dacă transferul datelor respective respectă cerințele prevăzute de RGPD și, după caz, pot sesiza instanțele naționale pentru ca acestea, dacă au îndoieli cu privire la validitatea deciziei Comisiei privind caracterul adecvat al nivelului de protecție, să adreseze Curții Europene de Justiție o cerere de pronunțare a unei hotărâri preliminare în vederea examinării validității.

[34] Cauza C-362/14 (Schrems I).

garanțiilor pe care le conțin cu măsuri suplimentare („măsuri suplimentare”), pentru a asigura un nivel de protecție în esență echivalent[35].

Derogările

24. Pe lângă deciziile privind caracterul adecvat al nivelului de protecție și instrumentele de transfer prevăzute la articolul 46 din RGPD, RGPD prevede o a treia cale care permite transferurile de date cu caracter personal în anumite situații. Sub rezerva unor condiții specifice, puteți transfera în continuare date cu caracter personal în temeiul unei derogări enumerate la articolul 49 din RGPD.

25. Articolul 49 din RGPD are un caracter excepțional. Derogările pe care le prevede trebuie interpretate în mod restrictiv și trebuie să se refere, în principal, la activități de prelucrare a datelor cu caracter personal care se desfășoară ocazional și nu sunt repetitive. CEPD a publicat Orientările 2/2018 privind derogările prevăzute la articolul 49 din Regulamentul (UE) 2016/679. [36]

26. Înainte de a invoca o derogare prevăzută la articolul 49 din RGPD, trebuie să verificați dacă transferurile dumneavoastră îndeplinesc condițiile stricte prevăzute de această dispoziție pentru fiecare dintre ele.

***

27. Dacă transferul dumneavoastră nu se poate întemeia din punct de vedere juridic pe o decizie privind caracterul adecvat al nivelului de protecție și nici pe o derogare prevăzută la articolul 49, trebuie să continuați cu cel de-al treilea pas.

2.3 Pasul 3: Evaluarea eficacității instrumentului de transfer prevăzut la articolul 46 din RGPD pe care vă bazați având în vedere toate circumstanțele transferului

28. Este posibil ca alegerea unui instrument de transfer prevăzut la articolul 46 din RGPD să nu fie suficientă. Instrumentul de transfer trebuie să asigure faptul că nivelul de protecție garantat de RGPD nu este subminat de transfer[37]. Cu alte cuvinte, instrumentul dumneavoastră de transfer trebuie să se aplice efectiv.

29. Prin „efectiv” se înțelege că datele cu caracter personal transferate beneficiază în țara terță de un nivel de protecție în esență echivalent cu cel garantat în SEE[38]. Acest lucru nu este valabil dacă importatorul de date este împiedicat să își respecte obligațiile ce îi revin în temeiul instrumentului de transfer, prevăzut la articolul 46 din RGPD pe care l-ați ales, dată fiind legislația și practicile țării terțe aplicabile transferului.

30. Prin urmare, trebuie să evaluați, dacă este necesar, în colaborare cu importatorul, dacă în legislația sau în practica țării terțe există vreun element care ar putea aduce atingere eficacității garanțiilor adecvate ale instrumentului de transfer prevăzut la articolul 46 din RGPD pe care vă bazați, în contextul transferului dumneavoastră specific. Dacă este necesar, importatorul dumneavoastră de date ar trebui să vă furnizeze sursele și informațiile relevante referitoare la țara terță în care este stabilit și la legislația

[35] C-311/18 (Schrems II), punctele 130 și 133. Vezi și punctul 2.3 de mai jos.
[36] Pentru mai multe informații privind acest aspect, vezi https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_ro.
[37] Articolul 44 din RGPD.
[38] C-311/18 (Schrems II), punctul 105 și a doua constatare.

aplicabilă transferului. De asemenea, puteți face trimitere la alte surse de informare, cum ar fi cele enumerate în mod neexhaustiv în anexa 3[39].

31. Evaluarea dumneavoastră ar trebui să ia în considerare toți actorii care participă la transfer (de exemplu, operatorii, persoanele împuternicite de operatori și subcontractanții care prelucrează date în țara terță), astfel cum au fost identificați în exercițiul de cartografiere a transferurilor. Cu cât sunt implicați mai mulți operatori, persoane împuternicite de operatori sau importatori, cu atât mai complexă va fi evaluarea dumneavoastră. De asemenea, în această evaluare va trebui să luați în considerare orice transfer ulterior care ar putea avea loc.

32. În acest scop, va trebui să analizați caracteristicile fiecăruia dintre transferurile dumneavoastră și să stabiliți modul în care se aplică acestor transferuri ordinea juridică internă a țării în care sunt transferate (sau transferate ulterior) datele.

33. Contextul juridic aplicabil va depinde de circumstanțele transferului, în special de:

- scopurile în care sunt transferate și prelucrate datele (de exemplu, comercializare, resurse umane, stocare, asistență TI, studii clinice);
- tipurile de entități implicate în prelucrare (publice/private, operator/persoană împuternicită de operator);
- sectorul în care are loc transferul (de exemplu, adtech, telecomunicații, financiar etc.);
- categoriile de date cu caracter personal transferate (de exemplu, datele cu caracter personal referitoare la copii pot intra sub incidența legislației specifice din țara terță);
- dacă datele vor fi stocate în țara terță sau dacă există doar acces de la distanță la datele stocate în UE/SEE;
- formatul datelor care urmează să fie transferate (adică, text simplu/pseudonimizat sau criptat[40]);
- posibilitatea ca datele să facă obiectul unor transferuri ulterioare din țara terță către o altă țară terță[41].

34. Dintre legile aplicabile, va trebui să evaluați dacă există vreo lege care aduce atingere angajamentelor cuprinse în instrumentul de transfer prevăzut la articolul 46 din RGPD pe care l-ați ales. Ar trebui să verificați dacă angajamentele care le permit persoanelor vizate să își exercite drepturile în contextul transferurilor internaționale (cum ar fi cererile de acces, de corectare și de ștergere a datelor transferate) pot fi aplicate efectiv și nu sunt împiedicate prin lege în țara terță de destinație.

35. Va trebui să evaluați normele relevante cu caracter general, în măsura în care acestea afectează aplicarea efectivă a garanțiilor cuprinse în instrumentul de transfer prevăzut la articolul 46 din RGPD și drepturile fundamentale ale persoanelor (în special, dreptul de a recurge la căi de atac de care dispune persoana vizată în cazul accesării datelor transferate de către autoritățile publice din țări terțe).

36. În orice caz, ar trebui să acordați o atenție deosebită oricăror legi relevante, în special legilor care stabilesc cerințe de comunicare a datelor cu caracter personal către autoritățile publice sau care acordă acestor autorități competențe de accesare a datelor cu caracter personal (de exemplu, în scopul

[39] Vezi și punctul 43 de mai jos.
[40] Unele țări terțe nu permit importul de date criptate.
[41] În cazul în care operatorul a acordat în prealabil autorizația scrisă, specifică sau generală, în conformitate cu articolul 28 alineatul (2) din RGPD.

asigurării respectării dreptului penal, al supravegherii normative și al securității naționale). Dacă aceste cerințe sau competențe se limitează la ceea ce este necesar și proporțional într-o societate democratică, [42]ele nu pot aduce atingere angajamentelor cuprinse în instrumentul de transfer prevăzut la articolul 46 din RGPD pe care vă bazați.

37. Standardele UE, cum ar fi articolele 47 și 52 din Carta drepturilor fundamentale a Uniunii Europene, trebuie utilizate ca referință pentru a evalua dacă un astfel de acces al autorităților publice este limitat la ceea ce este necesar și proporțional într-o societate democratică și dacă persoanele vizate beneficiază de căi de atac eficiente.

38. La efectuarea acestei evaluări, sunt relevante și diferite aspecte ale sistemului juridic din țara terță respectivă, de exemplu elementele enumerate la articolul 45 alineatul (2) din RGPD[43]. De exemplu, situația statului de drept dintr-o țară terță poate fi relevantă pentru evaluarea eficacității mecanismelor disponibile pentru ca persoanele să beneficieze de căi de atac (judiciare) împotriva accesului ilegal al guvernului la date cu caracter personal. Existența unei legislații detaliate cu privire la protecția datelor sau a unei autorități independente de protecție a datelor, precum și aderarea la instrumentele internaționale care prevăd garanții în materie de protecție a datelor, pot contribui la asigurarea proporționalității ingerinței guvernului[44].

***

39. Recomandările CEPD privind garanțiile esențiale europene (GEE) oferă elemente care trebuie evaluate pentru a se stabili dacă cadrul juridic care reglementează accesul autorităților publice dintr-o țară terță, fie acestea agenții naționale de securitate sau autorități de aplicare a legii, la datele cu caracter personal poate fi considerat sau nu o ingerință justificată (și, prin urmare, ca neaducând atingere angajamentelor asumate în instrumentul de transfer prevăzut la articolul 46 din RGPD). În special, acest lucru ar trebui analizat cu atenție atunci când legislația care reglementează accesul autorităților publice la date este ambiguă sau nu este disponibilă publicului.

40. Aplicate în cazul transferurilor de date în temeiul instrumentelor de transfer prevăzute la articolul 46, recomandările CEPD privind garanțiile esențiale europene pot îndruma exportatorul și importatorul de date în evaluarea faptului dacă aceste competențe constituie o ingerință nejustificată în obligațiile importatorului de date de a asigura echivalența esențială.

41. Lipsa unui nivel de protecție în esență echivalent se va observa în special în cazul în care legislația sau practica țării terțe relevantă pentru transferul dumneavoastră nu îndeplinește cerințele garanțiilor esențiale europene.

[42] Vezi articolele 47 și 52 din Carta drepturilor fundamentale a Uniunii Europene, articolul 23 alineatul (1) din RGPD și Recomandările 02/2020 privind garanțiile esențiale europene pentru măsurile de supraveghere, adoptate de CEPD la 10 noiembrie 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_ro.

[43] C-311/18 (Schrems II), punctul 104.

[44] De exemplu: Convenția 108 (Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, ETS nr. 108) sau Convenția 108+ (Convenția modernizată pentru protejarea persoanelor față de prelucrarea datelor cu caracter personal, CETS nr. 223) oferă căi de atac internaționale opozabile în cazul încălcării protecției datelor și contribuie la asigurarea unui nivel minim de protecție a datelor cu caracter personal și la respectarea vieții private.

42. Evaluarea dumneavoastră trebuie să se bazeze în primul rând pe legislația disponibilă publicului. Cu toate acestea, în anumite situații, acest lucru nu va fi suficient, deoarece este posibil ca legislația din țările terțe să lipsească. În acest caz, dacă încă mai doriți să efectuați transferul, ar trebui să analizați alți factori relevanți și obiectivi[45] și să nu vă bazați pe factori subiectivi, cum ar fi probabilitatea ca autoritățile publice să aibă acces la datele dumneavoastră într-un mod care contravine standardelor UE. Ar trebui să efectuați această evaluare cu diligența necesară și să o documentați temeinic, întrucât veți fi tras la răspundere pentru decizia pe care o puteți lua pe această bază[46].

43. Vă puteți completa evaluarea cu informații obținute din alte surse[47], cum ar fi:

- elemente care să demonstreze că o autoritate dintr-o țară terță va încerca să acceseze datele cu sau fără cunoștința importatorului de date, având în vedere precedentele, legislația și practicile raportate;
- elemente care să demonstreze că o autoritate dintr-o țară terță va putea accesa datele prin intermediul importatorului de date sau prin interceptarea directă a canalului de comunicare, având în vedere precedentele, competențele legale și resursele tehnice, financiare și umane de care dispune.

44. În cele din urmă, în evaluarea dumneavoastră puteți indica instrumentul de transfer prevăzut la articolul 46 din RGPD pe care vă bazați și garanțiile adecvate pe care le conține:

- garantează efectiv că datele cu caracter personal transferate beneficiază în țara terță de un nivel de protecție în esență echivalent cu cel garantat în SEE. Legislația și practicile țării terțe aplicabile transferului îi permit importatorului de date să își respecte obligațiile ce îi revin în temeiul instrumentului de transfer ales. Ar trebuie să efectuați o reevaluare la intervale corespunzătoare sau atunci când apar schimbări semnificative (vezi pasul 6).
- nu garantează efectiv un nivel de protecție în esență echivalent. Importatorul de date nu își poate respecta obligațiile, având în vedere legislația și/sau practicile țării terțe aplicabile transferului. CJUE a subliniat că, în cazul în care instrumentele de transfer prevăzute la articolul 46 din RGPD nu sunt suficiente, este responsabilitatea exportatorului de date fie să pună în aplicare măsuri suplimentare eficace, fie să nu transfere date cu caracter personal[48].

[45] Vezi punctul 43 de mai jos, precum și anexa 3.
[46] Articolul 5 alineatul (2) din RGPD.
[47] Vezi și anexa 3.
[48] CJUE C-311/18 (Schrems II), punctele 134-135.

CJUE a statuat, de exemplu, că secțiunea 702 din legea FISA a SUA nu respectă garanțiile minime care rezultă din principiul proporționalității prevăzut în dreptul Uniunii și nu poate fi considerată limitată la strictul necesar. Aceasta înseamnă că nivelul de protecție a programelor autorizate prin secțiunea 702 din FISA nu este, în esență, echivalent cu garanțiile impuse de dreptul Uniunii. În consecință, dacă importatorul de date sau orice alt destinatar căruia importatorul de date îi poate comunica datele intră sub incidența secțiunii 702 din FISA[49], CCS sau alte instrumente de transfer prevăzute la articolul 46 din RGPD pot fi invocate pentru un astfel de transfer numai dacă măsurile tehnice suplimentare fac imposibil sau ineficace accesul la datele transferate.

2.4 Pasul 4: Adoptarea de măsuri suplimentare

45. Dacă evaluarea de la pasul 3 a arătat că instrumentul dumneavoastră de transfer prevăzut la articolul 46 din RGPD nu este eficient, va trebui să analizați, dacă este necesar, în colaborare cu importatorul, dacă există măsuri suplimentare care, adăugate la garanțiile cuprinse în instrumentele de transfer, ar putea garanta că datele transferate beneficiază în țara terță de un nivel de protecție în esență echivalent cu cel garantat în UE[50]. „Măsurile suplimentare" sunt, prin definiție, suplimentare față de garanțiile pe care le oferă deja instrumentul de transfer prevăzut la articolul 46 din RGPD[51].

46. Trebuie să identificați, de la caz la caz, măsurile suplimentare care ar putea fi eficace pentru un set de transferuri către o anumită țară terță atunci când se utilizează un instrument de transfer specific prevăzut la articolul 46 din RGPD. Vă veți putea baza pe evaluările dumneavoastră anterioare de la pașii (1, 2 și 3 de mai sus) și veți putea verifica, ținând seama de constatările lor, eficacitatea potențială a măsurilor suplimentare în ceea ce privește garantarea nivelului de protecție necesar.

47. În principiu, măsurile suplimentare pot avea un caracter contractual, tehnic sau organizatoric. Combinarea diverselor măsuri într-un mod în care să se susțină și să se completeze reciproc poate îmbunătăți nivelul de protecție și, prin urmare, poate contribui la atingerea standardelor UE.

48. În general, doar măsurile contractuale și organizatorice nu vor restricționa accesul autorităților publice din țara terță la datele cu caracter personal (în cazul în care acest lucru constituie o ingerință nejustificată în obligațiile importatorului de date de a asigura echivalența esențială). Într-adevăr, vor exista situații în care numai măsurile tehnice ar putea împiedica sau lipsi de efect accesul autorităților publice din țările terțe la datele cu caracter personal, în special în scopuri de supraveghere[52]. În astfel de situații, măsurile contractuale sau organizatorice pot completa măsurile tehnice și pot consolida

[49] Secțiunea 702 din FISA se aplică dacă datele sunt obținute „de la un furnizor de servicii de comunicații electronice sau cu ajutorul acestuia" [secțiunea 702 din FISA = 50 USC § 1881a, la (h)(2)(A)(vi)], care, la rândul său, este definită în 50 USC § 1881(b)(4) ca
„(A) o societate de telecomunicații, astfel cum este definită în secțiunea 153 de la titlul 47;
(B) un furnizor de servicii de comunicații electronice, astfel cum este definit în secțiunea 2510 de la titlul 18;
(C) un furnizor de servicii informatice la distanță, astfel cum este definit în secțiunea 2711 de la titlul 18;
(D) orice alt furnizor de servicii de comunicații care are acces la comunicații prin cablu sau la comunicații electronice, astfel cum sunt transmise sau stocate aceste comunicații, sau
(E) un funcționar, un angajat sau un agent al unei entități descrise la litera (A), (B), (C) sau (D)."

[50] C-311/18 (Schrems II), punctul 96.

[51] Considerentul 109 din RGPD și C-311/18 (Schrems II), punctul 133.

[52] În cazul în care un astfel de acces depășește ceea ce este necesar și proporțional într-o societate democratică; vezi articolele 47 și 52 din Carta drepturilor fundamentale a Uniunii Europene, articolul 23 alineatul (1) din RGPD și Recomandările 02/2020 privind garanțiile esențiale europene pentru măsurile de supraveghere, adoptate de CEPD la 10 noiembrie 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_ro .

nivelul general de protecție a datelor, de exemplu prin crearea de obstacole în calea încercărilor autorităților publice de a accesa datele într-un mod care contravine standardelor UE.

49. Puteți, dacă este necesar, în colaborare cu importatorul de date, să consultați următoarea listă (neexhaustivă) de factori pentru a identifica cele mai eficace măsuri suplimentare pentru protejarea datelor transferate:

- formatul datelor care urmează să fie transferate (adică, text simplu/pseudonimizat sau criptat);
- natura datelor;
- lungimea și complexitatea fluxului de prelucrare a datelor, numărul de actori implicați în prelucrare și relația dintre ei [de exemplu, transferurile implică mai mulți operatori sau atât operatori, cât și persoane împuternicite de operatori sau implicarea persoanelor împuternicite de operatori care vor transfera datele de la dumneavoastră către importatorul dumneavoastră de date (luând în considerare dispozițiile relevante aplicabile acestora în temeiul legislației țării terțe de destinație)][53];
- Posibilitatea ca datele să facă obiectul unor transferuri ulterioare, în cadrul aceleiași țări terțe sau chiar către alte țări terțe (de exemplu, implicarea subcontractanților importatorului de date[54]).

Exemple de măsuri suplimentare

50. Câteva exemple de măsuri tehnice, contractuale și organizatorice care ar putea fi luate în considerare pot fi găsite în listele neexhaustive descrise în anexa 2.

***

51. Dacă ați pus în aplicare măsuri suplimentare eficace, care, împreună cu instrumentul de transfer prevăzut la articolul 46 din RGPD, ating un nivel de protecție în esență echivalent cu nivelul de protecție garantat în SEE: transferurile dumneavoastră pot avea loc.

52. În cazul în care nu puteți găsi sau pune în aplicare măsuri suplimentare eficace care să garanteze că datele cu caracter personal transferate beneficiază de un nivel de protecție în esență echivalent,[55] nu trebuie să începeți transferul de date cu caracter personal către țara terță în cauză în temeiul instrumentului de transfer prevăzut la articolul 46 din RGPD pe care vă bazați. Dacă efectuați deja transferuri, aveți obligația de a suspenda sau de a înceta imediat transferul de date cu caracter personal[56] . În conformitate cu garanțiile cuprinse în instrumentul de transfer prevăzut la articolul 46

[53] RGPD atribuie obligații distincte operatorilor și persoanelor împuternicite de operatori. Datele pot fi transferate de la operator la operator, între operatori asociați, de la operator la persoană împuternicită de operator și, sub rezerva autorizării de către operator, de la persoană împuternicită de operator la operator sau de la persoană împuternicită de operator la persoană împuternicită de operator.

[54] Vezi nota de subsol 25.

[55] În cazul în care un astfel de acces depășește ceea ce este necesar și proporțional într-o societate democratică; vezi articolele 47 și 52 din Carta drepturilor fundamentale a Uniunii Europene, articolul 23 alineatul (1) din RGPD și Recomandările 02/2020 privind garanțiile esențiale europene pentru măsurile de supraveghere, adoptate de CEPD la 10 noiembrie 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_ro .

[56] C-311/18 (Schrems II), punctul 135.

din RGPD pe care vă bazați, datele pe care le-ați transferat deja către țara terță respectivă și copiile lor ar trebui să fie în integralitate returnate sau distruse de către importator[57].

Exemplu: legislația țării terțe interzice măsurile suplimentare pe care le-ați identificat (de exemplu, interzice utilizarea criptării) sau subminează în alt mod eficacitatea acestora. Nu trebuie să începeți să transferați date cu caracter personal către această țară sau trebuie să încetați transferurile în curs către această țară.

53. Dacă decideți să continuați transferul, în pofida faptului că importatorul nu-și poate respecta angajamentele asumate în instrumentul de transfer prevăzut la articolul 46 din RGPD, trebuie să informați autoritatea de supraveghere competentă în conformitate cu dispozițiile specifice introduse în instrumentul de transfer relevant prevăzut la articolul 46 din RGPD[58]. Autoritatea de supraveghere competentă va suspenda sau va interzice transferurile de date în cazurile în care constată că nu se poate asigura un nivel de protecție în esență echivalent[59].

54. Autoritatea de supraveghere competentă poate impune alte măsuri corective (de exemplu, o amendă) dacă, în pofida faptului că nu puteți demonstra un nivel de protecție în esență echivalent în țara terță, începeți sau continuați transferul.

2.5 Pasul 5: Etapele procedurale în cazul în care ați identificat măsuri suplimentare eficace

55. Etapele procedurale pe care trebuie să le parcurgeți în cazul în care ați identificat măsuri suplimentare eficace care urmează să fie puse în aplicare pot varia în funcție de instrumentul de transfer prevăzut la articolul 46 din RGPD pe care îl utilizați sau intenționați să îl utilizați.

2.5.1 Clauze standard de protecție a datelor („CCS”) [articolul 46 alineatul (2) literele (c) și (d) din RGPD]

56. Atunci când, pe lângă CCS, intenționați să puneți în aplicare măsuri suplimentare, nu este necesar să solicitați o autorizație din partea autorității de supraveghere competente pentru a adăuga astfel de clauze sau garanții suplimentare, atât timp cât măsurile suplimentare identificate nu contravin, direct sau indirect, CCS și sunt suficiente pentru a garanta că nivelul de protecție garantat de RGPD nu este subminat[60]. Exportatorul și importatorul de date trebuie să se asigure că clauzele suplimentare nu pot

[57] Vezi clauza 12 din anexa la Decizia 87/2010 privind CCS; vezi clauza (opțională) de reziliere suplimentară din anexa B la Decizia 2004/915/CE privind CCS.

[58] Vezi Întrebări frecvente cu privire la hotărârea Curții de Justiție a Uniunii Europene în cauza C-311/18 - Data Protection Commissioner împotriva Facebook Ireland Ltd și Maximillian Schrems adoptate de CEPD la 23 iulie 2020, în special întrebările 5, 6 și 9. Vezi, de asemenea, clauza 4 litera (g) din Decizia 2010/87/UE a Comisiei, clauza 5 litera (a) din Decizia 2001/497/CE a Comisiei și clauza II litera (c) din anexa „Setul II” la Decizia 2004/915/CE a Comisiei.

[59] C-311/18 (Schrems II), punctele 113 și 121.

[60] Considerentul 109 din RGPD are următorul cuprins: „Posibilitatea ca operatorul sau persoana împuternicită de operator să utilizeze clauze standard în materie de protecție a datelor, adoptate de Comisie sau de o autoritate de supraveghere, nu ar trebui să împiedice operatorii sau persoanele împuternicite de aceștia să includă clauzele standard în materie de protecție a datelor într-un contract mai amplu, precum un contract între persoana împuternicită de operator și o altă persoană împuternicită de operator, și nici să adauge alte clauze sau garanții suplimentare, atât timp cât acestea nu contravin, direct sau indirect, clauzelor contractuale standard adoptate de Comisie sau de o autoritate de supraveghere sau nu prejudiciază drepturile sau libertățile fundamentale ale persoanelor vizate.” Dispoziții similare sunt prevăzute în seturile de CCS adoptate de Comisia Europeană în temeiul Directivei 95/45/CE.

fi interpretate în sensul restrângerii în vreun fel a drepturilor și obligațiilor din CCS sau al reducerii în orice alt fel a nivelului de protecție a datelor. Trebuie să puteți demonstra acest lucru, inclusiv lipsa de ambiguitate a tuturor clauzelor, în conformitate cu principiul responsabilității și cu obligația dumneavoastră de a asigura un nivel suficient de protecție a datelor. Autoritățile de supraveghere competente au competența de a revizui aceste clauze suplimentare atunci când este necesar (de exemplu, în cazul unei plângeri sau al unei anchete din proprie inițiativă).

57. În cazul în care intenționați să modificați clauzele standard de protecție a datelor sau în cazul în care măsurile suplimentare adăugate „contravin", direct sau indirect, CCS, se consideră că nu vă mai bazați pe clauze contractuale standard[61] și trebuie să solicitați o autorizație din partea autorității de supraveghere competente în conformitate cu articolul 46 alineatul (3) litera (a) din RGPD.

2.5.2 Reguli corporatiste obligatorii („BCR") [articolul 46 alineatul (2) litera (b) din RGPD]

58. Raționamentul prezentat în hotărârea Schrems II se aplică și altor instrumente de transfer în temeiul articolului 46 alineatul (2) din RGPD, deoarece toate aceste instrumente au, în esență, un caracter contractual, astfel încât garanțiile prevăzute și angajamentele asumate de părțile la acestea nu pot fi obligatorii pentru autoritățile publice din țări terțe[62].

59. Hotărârea Schrems II este relevantă pentru transferurile de date cu caracter personal în temeiul BCR, deoarece legislația țărilor terțe poate afecta protecția oferită de astfel de instrumente. Impactul real al hotărârii Schrems II asupra BCR este încă în discuție. CEPD va furniza cât mai curând posibil mai multe detalii cu privire la necesitatea includerii unor angajamente suplimentare în BCR din criteriile de referință WP256/257[63].

60. Curtea a subliniat că exportatorul și importatorul de date sunt cei care au responsabilitatea de a aprecia dacă nivelul de protecție impus de dreptul Uniunii este respectat în țara terță în cauză pentru a stabili dacă garanțiile oferite de CCS sau BCR pot fi efectiv respectate în practică. În caz contrar, ar trebui să verificați dacă puteți prevedea măsuri suplimentare pentru a asigura un nivel de protecție în esență echivalent cu cel prevăzut în cadrul SEE, precum și dacă legislația țării terțe în cauză nu va afecta aceste măsuri suplimentare în așa fel încât să submineze eficacitatea acestora.

[61] Vezi, prin analogie, Avizul nr. 17/2020 al CEPD privind proiectul de clauze contractuale standard înaintat de autoritatea de supraveghere din Slovenia [articolul 28 alineatul (8) din RGPD] cu privire la articolul 28 din SCC, adoptat deja, care conține o dispoziție similară („În plus, comitetul reamintește că posibilitatea de a utiliza clauzele contractuale standard adoptate de autoritatea de supraveghere nu împiedică părțile să adauge alte clauze sau garanții suplimentare, cu condiția ca acestea să nu contrazică, în mod direct sau indirect, clauzele contractuale standard adoptate sau să afecteze drepturile sau libertățile fundamentale ale persoanelor vizate. De asemenea, în cazul în care se modifică clauzele contractuale standard, nu se va mai considera că părțile au pus în aplicare clauzele contractuale standard adoptate."), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_ro.pdf.

[62] CJUE, C-311/18 (Schrems II), punctul 132.

[63] Grupul de lucru „Articolul 29", Document de lucru de stabilire a unui tabel cu elementele și principiile care trebuie să facă parte din regulile corporatiste obligatorii, astfel cum a fost cel mai recent revizuit și adoptat la 6 februarie 2018, WP 256 rev.01; Grupul de lucru „Articolul 29", Document de lucru de stabilire a unui tabel cu elementele și principiile care trebuie să facă parte din regulile corporatiste obligatorii, astfel cum a fost cel mai recent revizuit și adoptat la 6 februarie 2018, WP 257 rev.01.

2.5.3 Clauze contractuale ad-hoc [articolul 46 alineatul (3) litera (a) din RGPD]

61. Raționamentul prezentat în hotărârea Schrems II se aplică și altor instrumente de transfer în temeiul articolului 46 alineatul (2) din RGPD, deoarece toate aceste instrumente au, în esență, un caracter contractual, astfel încât garanțiile prevăzute și angajamentele asumate de părțile la acestea nu pot fi obligatorii pentru autoritățile publice din țări terțe[64]. Hotărârea Schrems II este, prin urmare, relevantă pentru transferurile de date cu caracter personal în temeiul unor clauze contractuale ad-hoc, deoarece legislația țărilor terțe poate afecta protecția oferită de aceste instrumente. Impactul real al hotărârii Schrems II asupra clauzelor ad-hoc este încă în discuție. CEPD va furniza mai multe detalii cât mai curând posibil.

2.6 Pasul 6: Reevaluarea la intervale corespunzătoare

62. Trebuie să monitorizați în permanență și, dacă este necesar, în colaborare cu importatorii de date, evoluțiile din țara terță către care ați transferat date cu caracter personal, care ar putea afecta evaluarea inițială a nivelului de protecție și posibilele decizii luate în consecință cu privire la transferurile dumneavoastră. Responsabilitatea este o obligație continuă [articolul 5 alineatul (2) din RGPD].

63. Ar trebui să puneți în aplicare mecanisme suficient de solide pentru a vă asigura că suspendați sau încetați imediat transferurile în cazul în care:

- importatorul și-a încălcat sau nu-și poate onora angajamentele asumate în instrumentul de transfer prevăzut la articolul 46 din RGPD sau
- măsurile suplimentare nu mai au efect în țara terță în cauză.

[64] CJUE, C-311/18 (Schrems II), punctul 132.

CONCLUZIE

64. RGPD stabilește norme privind prelucrarea datelor cu caracter personal în SEE, permițând astfel libera circulație a datelor cu caracter personal în cadrul SEE. Capitolul V din RGPD reglementează transferurile de date cu caracter personal către țări terțe și stabilește un standard înalt: transferul nu trebuie să submineze nivelul de protecție a persoanelor fizice garantat de RGPD (articolul 44 din RGPD). Hotărârea CJUE C-311/18 (Schrems II) subliniază necesitatea de a asigura continuitatea nivelului de protecție de care beneficiază datele cu caracter personal transferate către o țară terță în temeiul RGPD[65].

65. Pentru a asigura un nivel în esență echivalent de protecție a datelor dumneavoastră, trebuie să cunoașteți în primul rând toate detaliile transferurilor. De asemenea, trebuie să verificați dacă datele pe care le transferați sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt transferate și prelucrate în țara terță.

66. De asemenea, trebuie să identificați instrumentul de transfer pe care vă bazați pentru transferuri. Dacă instrumentul de transfer nu este o decizie privind caracterul adecvat al nivelului de protecție, trebuie să verificați, de la caz la caz, dacă legislația sau practica țării terțe de destinație subminează (sau nu) garanțiile cuprinse în instrumentul de transfer prevăzut la articolul 46 din RGPD în contextul transferurilor dumneavoastră. În cazul în care instrumentul de transfer prevăzut la articolul 46 din RGPD nu reușește să obțină singur un nivel de protecție în esență echivalent pentru datele cu caracter personal pe care le transferați, măsurile suplimentare pot acoperi lacunele.

67. În cazul în care nu puteți găsi sau pune în aplicare măsuri suplimentare eficace care să asigure că datele cu caracter personal transferate beneficiază de un nivel de protecție în esență echivalent, nu trebuie să începeți transferul de date cu caracter personal către țara terță în cauză în temeiul instrumentului de transfer ales de dumneavoastră. Dacă efectuați deja transferuri, aveți obligația de a suspenda sau de a înceta imediat transferul de date cu caracter personal.

68. Autoritatea de supraveghere competentă are competența de a suspenda sau de a înceta transferurile de date cu caracter personal către țara terță dacă nu este asigurată protecția datelor transferate impusă de dreptul UE, în special articolele 45 și 46 din RGPD și Carta drepturilor fundamentale.

Pentru Comitetul european pentru protecția datelor

Președinte

(Andrea Jelinek)

[65] C-311/18 (Schrems II), punctul 93.

ANEXA 1: DEFINIȚII

- „Țară terță” înseamnă orice țară care nu este stat membru al SEE.
- „SEE” înseamnă Spațiul Economic European și include statele membre ale Uniunii Europene și Islanda, Norvegia și Liechtenstein. RGPD se aplică acestora din urmă în temeiul Acordului privind SEE, în special al anexei XI și al Protocolului 37 la acesta.
- Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).
- „Carta” se referă la Carta drepturilor fundamentale a Uniunii Europene, JO C 326, 26.10.2012, p. 391-407.
- „CJUE” sau „Curtea” se referă la Curtea de Justiție a Uniunii Europene. Aceasta constituie autoritatea judiciară a Uniunii Europene și, în cooperare cu instanțele statelor membre, asigură aplicarea și interpretarea uniformă a dreptului Uniunii.
- „Exportator de date” înseamnă operatorul sau persoana împuternicită de operator din cadrul SEE care transferă date cu caracter personal unui operator sau unei persoane împuternicite de operator dintr-o țară terță.
- „Importator de date” înseamnă operatorul sau persoana împuternicită de operator dintr-o țară terță care primește sau obține acces la datele cu caracter personal transferate din SEE.
- „Instrumentul de transfer prevăzut la articolul 46 din RGPD” se referă la garanțiile adecvate prevăzute la articolul 46 din RGPD pe care exportatorii de date trebuie să le pună în aplicare atunci când transferă date cu caracter personal către o țară terță, în absența unei decizii privind caracterul adecvat al nivelului de protecție în temeiul articolului 45 alineatul (3) din RGPD. Articolul 46 alineatele (2) și (3) din RGPD conține lista instrumentelor de transfer prevăzute la articolul 46 din RGPD pe care operatorii și persoanele împuternicite de operatori le pot utiliza.
- „CCS” înseamnă clauzele standard de protecție a datelor (sau „clauzele contractuale standard”) adoptate de Comisia Europeană pentru transferuri de date cu caracter personal între operatori sau persoane împuternicite de operatori din SEE și operatori sau persoane împuternicite de operatori din afara SEE. Clauzele contractuale standard adoptate de Comisia Europeană sunt un instrument de transfer în temeiul RGPD, în conformitate cu articolul 46 alineatul (2) litera (c) și alineatul (5) din RGPD.

ANEXA 2: EXEMPLE DE MĂSURI SUPLIMENTARE

69. Următoarele măsuri sunt exemple de măsuri suplimentare pe care le puteți lua în considerare atunci când ajungeți la pasul 4 „Adoptarea de măsuri suplimentare”. Această listă nu este exhaustivă. Selectarea și punerea în aplicare a uneia sau a mai multora dintre aceste măsuri nu vor garanta în mod obligatoriu și sistematic faptul că transferul dumneavoastră îndeplinește standardul de echivalență esențială impus de dreptul UE. Ar trebui să selectați măsurile suplimentare care pot garanta efectiv acest nivel de protecție pentru transferurile dumneavoastră.

70. Orice măsură suplimentară poate fi considerată eficace în sensul hotărârii CJUE „Schrems II” numai dacă și în măsura în care aceasta abordează deficiențele specifice identificate în evaluarea situației juridice din țara terță. Dacă, în cele din urmă, nu puteți asigura un nivel de protecție în esență echivalent, nu trebuie să transferați datele cu caracter personal.

71. În calitate de operator sau persoană împuternicită de operator, este posibil să aveți deja obligația să puneți în aplicare unele dintre măsurile descrise în prezenta anexă, chiar dacă importatorul dumneavoastră de date face obiectul unei decizii privind caracterul adecvat al nivelului de protecție, după cum este posibil să aveți obligația să le puneți în aplicare atunci când prelucrați datele în cadrul SEE[66].

Măsuri tehnice

72. Prezenta secțiune descrie în mod neexhaustiv exemple de măsuri tehnice, care pot completa garanțiile cuprinse în instrumentele de transfer prevăzute la articolul 46 din RGPD pentru a asigura respectarea nivelului de protecție impus de dreptul UE în contextul unui transfer de date cu caracter personal către o țară terță. Aceste măsuri vor fi necesare în special în cazul în care legislația țării respective impune importatorilor de date obligații care sunt contrare garanțiilor cuprinse în instrumentele de transfer prevăzute la articolul 46 din RGPD și care, în special, pot afecta garanția contractuală a unui nivel de protecție în esență echivalent împotriva accesului autorităților publice ale țării terțe în cauză la datele respective[67].

73. Pentru mai multă claritate, prezenta secțiune specifică, în primul rând, măsurile tehnice care ar putea fi eficace în anumite scenarii/cazuri de utilizare pentru a asigura un nivel de protecție în esență echivalent. Secțiunea continuă cu unele scenarii/cazuri de utilizare în care nu au putut fi găsite măsuri tehnice care să asigure acest nivel de protecție.

Scenarii pentru care ar putea fi găsite măsuri *eficace*

74. Măsurile enumerate mai jos sunt menite să asigure faptul că accesul autorităților publice din țările terțe la datele transferate nu aduce atingere eficacității garanțiilor adecvate ale instrumentelor de transfer prevăzute la articolul 46 din RGPD. Aceste măsuri se aplică chiar dacă accesul autorităților publice respectă legislația țării importatorului, în cazul în care un astfel de acces depășește ceea ce este necesar și proporțional într-o societate democratică[68]. Aceste măsuri urmăresc să împiedice

[66] Articolul 5 alineatul (2) din RGPD, articolul 32 din RGPD.
[67] C-311/18 (Schrems II), punctul 135.
[68] Vezi articolele 47 și 52 din Carta drepturilor fundamentale a Uniunii Europene, articolul 23 alineatul (1) din RGPD și Recomandările CEPD privind garanțiile esențiale europene pentru măsurile de supraveghere.

posibila încălcare a accesului la date prin împiedicarea autorităților de a identifica persoanele vizate, de a deduce informații despre acestea, de a le individualiza într-un alt context sau de a asocia datele transferate cu alte seturi de date pe care le pot deține și care pot conține, printre alte date, identificatori online furnizați de dispozitive, aplicații, instrumente și protocoale utilizate de persoanele vizate în alte contexte.

75. Autoritățile publice din țările terțe pot încerca să acceseze datele transferate

a) în tranzit prin accesarea liniilor de comunicare utilizate pentru transmiterea datelor către țara destinatară. Acest acces poate fi pasiv, caz în care conținutul comunicării, posibil în urma unui proces de selecție, este pur și simplu copiat. Cu toate acestea, accesul poate fi și activ în sensul că autoritățile publice se interpun în procesul de comunicare nu numai prin citirea conținutului, ci și prin manipularea sau eliminarea unor părți din acesta.

b) atunci când se află în custodia unui destinatar preconizat al datelor, fie accesând instalațiile de prelucrare propriu-zise, fie solicitând unui destinatar al datelor să localizeze și să extragă date de interes și să le transfere autorităților.

76. Această secțiune analizează scenariile în care se aplică măsuri eficace în ambele cazuri. Se pot aplica măsuri suplimentare diferite care pot fi suficiente în situația dată a unui transfer concret, în cazul în care legislația țării destinatare prevede doar un singur tip de acces. Prin urmare, este necesar ca exportatorul de date să analizeze cu atenție, cu sprijinul importatorului de date, obligațiile ce îi revin acestuia din urmă.

De exemplu, importatorii de date din SUA care intră sub incidența articolului 50 USC § 1881a (secțiunea 702 din FISA) au obligația directă de a acorda acces la datele cu caracter personal importate care se află în posesia, custodia sau controlul lor sau de a le preda. Această obligație se poate extinde la orice chei criptografice necesare pentru ca datele să devină inteligibile.

77. Scenariile descriu circumstanțele specifice și măsurile luate. Orice modificare a scenariilor poate conduce la concluzii diferite.

78. Este posibil ca operatorii să fie nevoiți să aplice unele măsuri sau toate măsurile descrise aici, indiferent de nivelul de protecție prevăzut de legislația aplicabilă importatorului de date, deoarece acestea sunt necesare pentru a respecta articolele 25 și 32 din RGPD în circumstanțele concrete ale transferului. Cu alte cuvinte, exportatorii pot avea obligația să pună în aplicare măsurile descrise în prezentul document, chiar dacă importatorii de date ai acestora fac obiectul unei decizii privind caracterul adecvat al nivelului de protecție, după cum operatorii și persoanele împuternicite de operatori pot avea obligația să le pună în aplicare atunci când datele sunt prelucrate în cadrul SEE.

Cazul de utilizare 1: Stocarea datelor în scopul creării de copii de rezervă și în alte scopuri care nu necesită acces la date necriptate

79. Un exportator de date utilizează un furnizor de servicii de găzduire dintr-o țară terță pentru a stoca date cu caracter personal, de exemplu, în scopul creării de copii de rezervă.

Dacă

1. datele cu caracter personal sunt prelucrate utilizând algoritmi de criptare puternici înainte de transmitere;

2. algoritmul de criptare și parametrizarea acestuia (de exemplu, lungimea cheii, modul de operare, dacă este cazul) sunt conforme cu stadiul actual al tehnologiei și pot fi considerate solide în raport cu criptanaliza efectuată de autoritățile publice din țara destinatară, ținând seama de resursele și capacitățile tehnice (de exemplu, puterea de calcul în caz de atacuri brutale) de care dispun;
3. puterea criptării ia în considerare perioada specifică în care trebuie păstrată confidențialitatea datelor cu caracter personal criptate;
4. algoritmul de criptare este pus în aplicare fără erori de un software întreținut corespunzător, a cărui conformitate cu specificațiile algoritmului ales a fost verificată, de exemplu, prin certificare;
5. cheile sunt gestionate (generate, administrate, stocate, dacă este cazul, asociate identității destinatarului preconizat și revocate) în mod fiabil; și
6. cheile sunt păstrate exclusiv sub controlul exportatorului de date sau al altor entități cărora le-a fost încredințată această sarcină care își au reședința în SEE sau într-o țară terță, pe un teritoriu ori într-unul sau mai multe sectoare specificate dintr-o țară terță sau la o organizație internațională în privința cărora Comisia a stabilit, în conformitate cu articolul 45 din RGPD, că asigură un nivel de protecție adecvat;

în concluzie, CEPD consideră că criptarea efectuată constituie o măsură suplimentară eficace.

Cazul de utilizare 2: Transferul de date pseudonimizate

80. Un exportator de date pseudonimizează mai întâi datele pe care le deține și apoi le transferă către o țară terță pentru analiză, de exemplu, în scopuri de cercetare.

Dacă

1. un exportator de date transferă date cu caracter personal prelucrate în așa fel încât acestea să nu mai poată fi atribuite unei anume persoane vizate și nici să nu poată fi utilizate pentru a individualiza persoana vizată într-un grup mai mare, fără a se utiliza informații suplimentare[69];
2. informațiile suplimentare sunt deținute exclusiv de exportatorul de date și păstrate separat într-un stat membru sau într-o țară terță, pe un teritoriu ori într-unul sau mai multe sectoare specificate dintr-o țară terță sau la o organizație internațională în privința cărora Comisia a stabilit, în conformitate cu articolul 45 din RGPD, că asigură un nivel de protecție adecvat;
3. divulgarea sau utilizarea neautorizată a informațiilor suplimentare respective este împiedicată de garanții tehnice și organizatorice adecvate, se asigură faptul că exportatorul de date deține controlul exclusiv asupra algoritmului sau a depozitului care permite reidentificarea utilizând informațiile suplimentare și
4. operatorul a stabilit, prin intermediul unei analize aprofundate a datelor în cauză, ținând seama de orice informații pe care autoritățile publice din țara destinatară le pot deține, că datele cu caracter personal pseudonimizate nu pot fi atribuite unei persoane fizice identificate sau identificabile, chiar dacă se face trimitere încrucișată la acestea;

în concluzie, CEPD consideră că pseudonimizarea efectuată constituie o măsură suplimentară eficace.

[69] În conformitate cu articolul 4 alineatul (5) din RGPD: „«pseudonimizare» înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;”

81. Trebuie remarcat faptul că, în multe situații, elementele specifice identității fizice, fiziologice, genetice, psihice, economice, culturale sau sociale a unei persoane fizice, localizarea sa fizică sau interacțiunea acesteia cu un serviciu bazat pe internet în anumite momente în timp[70] pot permite identificarea persoanei respective chiar dacă numele, adresa sau alți identificatori simpli ai acesteia sunt omise.

82. Acest lucru este valabil în special atunci când datele se referă la utilizarea serviciilor de informare (momentul accesării, secvența de caracteristici accesate, caracteristicile dispozitivului utilizat etc.). Aceste servicii ar putea foarte bine, la fel ca în cazul importatorului de date cu caracter personal, avea obligația de a acorda acces acelorași autorități publice din jurisdicția lor, care vor deține probabil date cu privire la utilizarea acestor servicii de informare de către persoana (persoanele) vizată (vizate).

83. În plus, dat fiind că utilizarea anumitor servicii de informare este, prin natura sa, publică sau că acestea pot fi exploatate de către părți cu resurse substanțiale, operatorii vor trebui să fie mult mai atenți, având în vedere faptul că autoritățile publice din jurisdicția lor dețin probabil date cu privire la utilizarea serviciilor de informare de către o persoană vizată.

Cazul de utilizare 3: Date criptate care doar tranzitează țările terțe

84. Un exportator de date dorește să transfere date către o destinație recunoscută ca oferind o protecție adecvată în conformitate cu articolul 45 din RGPD. Datele sunt direcționate către o țară terță.

Dacă

1. un exportator de date transferă date cu caracter personal către un importator de date dintr-o jurisdicție care asigură o protecție adecvată, datele sunt transmise prin internet, acestea putând fi direcționate geografic printr-o țară terță care nu oferă un nivel de protecție în esență echivalent;
2. este utilizată criptarea transmisiei pentru care se asigură protocoale de criptare de ultimă generație care oferă o protecție eficace împotriva atacurilor active și pasive, cu resurse cunoscute a fi disponibile autorităților publice din țara terță;
3. decriptarea este posibilă numai în afara țării terțe în cauză;
4. părțile implicate în comunicare convin asupra unei infrastructuri sau a unei autorități credibile de certificare cu cheie publică;
5. sunt utilizate măsuri specifice de protecție și de ultimă generație împotriva atacurilor active și pasive asupra transmisiilor criptate;
6. în cazul în care criptarea transmisiei nu oferă în sine o securitate adecvată din cauza experienței legate de vulnerabilitățile infrastructurii sau ale software-ului utilizat, datele cu caracter personal sunt, de asemenea, criptate de la un capăt la altul la nivelul aplicației utilizând metode de criptare de ultimă generație;
7. algoritmul de criptare și parametrizarea acestuia (de exemplu, lungimea cheii, modul de operare, dacă este cazul) sunt conforme cu stadiul actual al tehnologiei și pot fi considerate solide în raport cu criptanaliza efectuată de autoritățile publice din țara de tranzit, ținând seama de resursele și capacitățile tehnice (de exemplu, puterea de calcul în caz de atacuri brutale) de care dispun;
8. puterea criptării ia în considerare perioada specifică în care trebuie păstrată confidențialitatea datelor cu caracter personal criptate;

[70] Articolul 4 alineatul (1) din RGPD: „«date cu caracter personal» înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;”.

9. algoritmul de criptare este pus în aplicare fără erori de un software întreținut corespunzător, a cărui conformitate cu specificațiile algoritmului ales a fost verificată, de exemplu, prin certificare;
10. a fost exclusă existența unor uși secrete (în hardware sau software);
11. cheile sunt gestionate (generate, administrate, stocate, dacă este cazul, asociate identității destinatarului preconizat și revocate) în mod fiabil de către exportator sau de către o entitate în care exportatorul are încredere într-o jurisdicție care oferă un nivel de protecție în esență echivalent;

în concluzie, CEPD consideră că criptarea transmisiei, dacă este necesar, în combinație cu criptarea conținutului de la un capăt la altul, constituie o măsură suplimentară eficace.

Cazul de utilizare 4: Destinatar protejat

85. Un exportator de date transferă date cu caracter personal către un importator de date dintr-o țară terță protejată în mod specific de legislația țării respective, de exemplu, pentru a oferi în comun tratament medical unui pacient sau servicii juridice unui client.

Dacă

1. legislația unei țări terțe exonerează importatorul de date rezident de răspundere în ceea ce privește posibila încălcare a accesului la datele deținute de destinatarul respectiv într-un anumit scop, de exemplu, în virtutea obligației de păstrare a secretului profesional care se aplică importatorului de date;
2. această exonerare se extinde la toate informațiile aflate în posesia importatorului de date, care pot fi utilizate pentru a eluda protecția informațiilor privilegiate (chei criptografice, parole, alte acreditări etc.);
3. importatorul de date nu utilizează serviciile unei persoane împuternicite de operator într-un mod care să permită autorităților publice să acceseze datele deținute de persoana împuternicită de operator și nici nu transmite datele unei alte entități care nu este protejată, în temeiul instrumentelor de transfer prevăzute la articolul 46 din RGPD;
4. datele cu caracter personal sunt criptate înainte de a fi transmise printr-o metodă conformă cu stadiul actual al tehnologiei, care garantează că decriptarea nu va fi posibilă fără cunoașterea cheii de decriptare (criptare de la un capăt la altul) pe toată perioada în care datele trebuie protejate;
5. cheia de decriptare se află în custodia exclusivă a importatorului de date protejat și este securizată în mod corespunzător împotriva utilizării sau divulgării neautorizate prin măsuri tehnice și organizatorice conforme cu stadiul actual al tehnologiei; și
6. exportatorul de date a stabilit în mod fiabil că cheia de criptare pe care intenționează să o utilizeze corespunde cheii de decriptare deținute de destinatar;

în consecință, CEPD consideră că criptarea transmisiei efectuată constituie o măsură suplimentară eficace.

Cazul de utilizare 5: Prelucrarea fracționată sau multipartită

86. Exportatorul de date dorește ca datele cu caracter personal să fie prelucrate în comun de către două sau mai multe persoane independente împuternicite de operator, situate în jurisdicții diferite, fără a le divulga conținutul datelor. Înainte de a transmite datele, acesta le împarte astfel încât nicio parte pe care o primește o persoană împuternicită de operator să nu conțină suficiente elemente pentru reconstituirea, în tot sau în parte, a datelor cu caracter personal. Exportatorul de date primește

rezultatul prelucrării de la fiecare dintre persoanele împuternicite de operator și unifică elementele primite pentru a ajunge la rezultatul final care poate constitui datele cu caracter personal sau agregate.

Dacă

1. un exportator de date prelucrează datele cu caracter personal astfel încât acestea să fie împărțite în două sau mai multe părți, fiecare dintre acestea nemaiputând fi interpretate sau atribuite unei anumite persoane vizate, fără a se utiliza informații suplimentare;
2. fiecare dintre părți este transferată unei persoane separate împuternicite de operator, situată într-o altă jurisdicție;
3. persoanele împuternicite de operator prelucrează opțional datele în comun, de exemplu utilizând un calcul multipartit securizat, astfel încât niciuneia dintre ele să nu îi fie dezvăluită nicio informație pe care nu o deținea înainte de efectuarea calculului;
4. algoritmul utilizat pentru calculul partajat este securizat împotriva adversarilor activi;
5. nu există nicio dovadă de colaborare între autoritățile publice situate în jurisdicțiile în care se află fiecare dintre persoanele împuternicite de operator, care le-ar permite acestora accesul la toate seturile de date cu caracter personal deținute de persoanele împuternicite de operator, precum și să reconstituie și să exploateze conținutul datelor cu caracter personal într-o formă clară, în circumstanțe în care o astfel de exploatare nu ar respecta esența drepturilor și libertăților fundamentale ale persoanelor vizate. În mod similar, autoritățile publice din oricare dintre aceste țări nu ar trebui să aibă autoritatea de a accesa datele cu caracter personal deținute de persoanele împuternicite de operator în toate jurisdicțiile în cauză;
6. operatorul a stabilit, prin intermediul unei analize aprofundate a datelor în cauză, ținând seama de orice informații pe care autoritățile publice din țările destinatare le pot deține, că datele cu caracter personal pe care le transmite persoanelor împuternicite de operator nu pot fi atribuite unei persoane fizice identificate sau identificabile, chiar dacă se face trimitere încrucișată la acestea;

în consecință, CEPD consideră că prelucrarea fracționată efectuată constituie o măsură suplimentară eficace.

Scenarii în care *nu* ar putea fi găsite măsuri eficace

87. Măsurile descrise mai jos în cadrul anumitor scenarii nu ar fi eficace în ceea ce privește asigurarea unui nivel de protecție în esență echivalent pentru datele transferate către țara terță. Prin urmare, acestea nu s-ar califica drept măsuri suplimentare.

Cazul de utilizare 6: Transferul către furnizorii de servicii de cloud sau alte persoane împuternicite de operator care necesită acces la date necriptate

88. Un exportator de date utilizează un furnizor de servicii de cloud sau o altă persoană împuternicită de operator pentru ca datele cu caracter personal să fie prelucrate în conformitate cu instrucțiunile sale într-o țară terță.

Dacă

1. un operator transferă date către un furnizor de servicii de cloud sau către altă persoană împuternicită de operator;

2. furnizorul de servicii de cloud sau altă persoană împuternicită de operator are nevoie de acces la date necriptate pentru a executa sarcina încredințată; și
3. competența acordată autorităților publice din țara destinatară de a accesa datele transferate depășește ceea ce este necesar și proporțional într-o societate democratică[71];

în consecință, având în vedere stadiul actual al tehnologiei, CEPD nu poate să prevadă o măsură tehnică eficace pentru a împiedica încălcarea drepturilor persoanelor vizate printr-un astfel de acces. CEPD nu exclude posibilitatea ca evoluțiile tehnologice viitoare să ofere măsuri care să atingă obiectivele de afaceri avute în vedere, fără a solicita acces necriptat.

89. În scenariile date, atunci când din punct de vedere tehnic sunt necesare date cu caracter personal necriptate pentru furnizarea serviciului de către persoana împuternicită de operator, criptarea transmisiei și criptarea datelor inactive, chiar luate împreună, nu constituie o măsură suplimentară care asigură un nivel de protecție în esență echivalent în cazul în care importatorul de date se află în posesia cheilor criptografice.

Cazul de utilizare 7: Accesul de la distanță la date în scopuri comerciale

90. Un exportator de date pune la dispoziția entităților dintr-o țară terță date cu caracter personal pentru a fi utilizate în scopuri comerciale comune. O combinație tipică poate consta dintr-un operator sau o persoană împuternicită de operator stabilită pe teritoriul unui stat membru care transferă date cu caracter personal către un operator sau o persoană împuternicită de operator dintr-o țară terță care face parte din același grup de întreprinderi sau din același grup de întreprinderi implicate într-o activitate economică comună. Importatorul de date poate, de exemplu, să utilizeze datele pe care le primește pentru a furniza servicii legate de personal exportatorului de date, pentru care are nevoie de date privind resursele umane, sau pentru a comunica prin telefon sau e-mail cu clienții exportatorului de date care locuiesc în Uniunea Europeană.

Dacă

1. un exportator de date transferă date cu caracter personal către un importator de date dintr-o țară terță, punându-le la dispoziție într-un sistem de informații utilizat în mod curent într-un mod care să îi permită importatorului accesul direct la datele pe care le dorește, sau transferându-le direct, individual sau în vrac, prin utilizarea unui serviciu de comunicații;
2. importatorul utilizează datele necriptate în scopuri proprii;
3. competența acordată autorităților publice din țara destinatară de a accesa datele transferate depășește ceea ce este necesar și proporțional într-o societate democratică;

în acest caz, CEPD nu poate să prevadă o măsură tehnică eficace pentru a împiedica încălcarea drepturilor persoanelor vizate printr-un astfel de acces.

91. În scenariile date, atunci când din punct de vedere tehnic sunt necesare date cu caracter personal necriptate pentru furnizarea serviciului de către persoana împuternicită de operator, criptarea transmisiei și criptarea datelor inactive, chiar luate împreună, nu constituie o măsură suplimentară care asigură un nivel de protecție în esență echivalent în cazul în care importatorul de date se află în posesia cheilor criptografice.

[71] Vezi articolele 47 și 52 din Carta drepturilor fundamentale a Uniunii Europene, articolul 23 alineatul (1) din RGPD și Recomandările CEPD privind garanțiile esențiale europene pentru măsurile de supraveghere.

Măsuri contractuale suplimentare

92. Aceste măsuri vor consta, în general, în angajamente contractuale[72] unilaterale, bilaterale sau multilaterale[73] . Dacă se utilizează un instrument de transfer prevăzut la articolul 46 din RGPD, în majoritatea cazurilor, acesta va cuprinde deja o serie de angajamente (în principal contractuale) ale exportatorului și importatorului de date, menite să servească drept garanții pentru datele cu caracter personal[74].

93. În unele situații, aceste măsuri pot completa și consolida garanțiile pe care le pot prevedea instrumentul de transfer și legislația relevantă a țării terțe, atunci când, ținând seama de circumstanțele transferului, acestea nu îndeplinesc toate condițiile necesare pentru a asigura un nivel de protecție în esență echivalent cu cel garantat în cadrul UE. Dată fiind natura măsurilor contractuale, care, în general, nu pot fi obligatorii pentru autoritățile din țara terță în cauză, atunci când acestea nu sunt părți la contract[75], aceste măsuri ar trebui să fie combinate cu alte măsuri tehnice și organizatorice pentru a asigura nivelul necesar de protecție a datelor. Selectarea și punerea în aplicare a uneia sau a mai multora dintre aceste măsuri nu vor garanta în mod obligatoriu și sistematic faptul că transferul dumneavoastră îndeplinește standardul de echivalență esențială impus de dreptul UE.

94. În funcție de măsurile contractuale deja cuprinse în instrumentul de transfer prevăzut la articolul 46 din RGPD care este invocat, măsurile contractuale suplimentare pot fi, de asemenea, utile în a permite exportatorilor de date din cadrul SEE să se informeze în legătură cu noile evoluții care afectează protecția datelor transferate către țări terțe.

95. După cum s-a menționat anterior, măsurile contractuale nu vor putea exclude aplicarea legislației unei țări terțe care nu respectă standardul CEPD cu privire la garanțiile esențiale europene în cazurile în care legislația obligă importatorii să respecte ordinele de comunicare a datelor pe care le primesc de la autoritățile publice[76].

96. Câteva exemple de posibile măsuri contractuale sunt enumerate mai jos și clasificate în funcție de natura lor:

Prevederea obligației contractuale de a utiliza măsuri tehnice specifice

97. ***În funcție de circumstanțele specifice ale transferurilor, pentru ca acestea să aibă loc, ar putea fi necesar să se prevadă în contract punerea în aplicare a unor măsuri tehnice specifice (vezi mai sus măsurile tehnice sugerate).***

[72] Acestea vor avea un caracter privat și nu vor fi considerate acorduri internaționale în temeiul dreptului internațional public. În consecință, în mod normal, acestea nu vor fi obligatorii pentru autoritatea publică a țării terțe, întrucât aceasta din urmă nu este parte la contractul încheiat cu organismele private ale țării terțe, astfel cum a subliniat Curtea la punctul 125 din hotărârea sa C-311/18 (Schrems II).

[73] De exemplu, în cadrul BCR care ar trebui, în orice caz, să reglementeze unele dintre măsurile enumerate mai jos.

[74] Vezi hotărârea C-311/18 (Schrems II), punctul 137, în care Curtea a recunoscut, în consecință, că CCS cuprinde *„mecanisme eficiente care permit, în practică, să se asigure respectarea nivelului de protecție impus de dreptul Uniunii și suspendarea sau interzicerea transferurilor de date cu caracter personal, întemeiate pe astfel de clauze, în cazul încălcării acestor clauze sau al imposibilității de a le onora”*; vezi și punctul 148).

[75] C-311/18 (Schrems II), punctul 125.

[76] Hotărârea CJUE C-311/18 (Schrems II), punctul 132.

98. ***Condiții de eficacitate:***

- Această clauză ar putea fi eficace în situațiile în care exportatorul a identificat necesitatea adoptării unor măsuri tehnice. În acest caz, aceasta ar trebui să fie transpusă într-o formă juridică pentru a se asigura că și importatorul se angajează să pună în aplicare măsurile tehnice necesare, dacă este cazul.

Obligații de transparență:

99. ***Exportatorul ar putea adăuga anexe la contract cu informații pe care importatorul ar face tot posibilul să le furnizeze, privind accesul autorităților publice la date, inclusiv în domeniul serviciilor de informații, cu condiția ca legislația să respecte garanțiile esențiale europene ale CEPD, în țara de destinație. Acest lucru ar putea ajuta exportatorul de date să își îndeplinească obligația de documentare a evaluării nivelului de protecție în țara terță.***

100. De exemplu, importatorul ar putea avea obligația:

(1) să enumere actele cu putere de lege și normele administrative din țara de destinație aplicabile importatorului sau persoanelor împuternicite de operator (subcontractanților) care ar permite accesul autorităților publice la datele cu caracter personal care fac obiectul transferului, în special în domeniul serviciilor de informații, al aplicării legii, al supravegherii administrative și normative aplicabile datelor transferate;
(2) în absența unor legi care să reglementeze accesul autorităților publice la date, să furnizeze informații și statistici pe baza experienței importatorului sau a rapoartelor din diverse surse (de exemplu, parteneri, surse deschise, jurisprudență națională și decizii ale organismelor de supraveghere) privind accesul autorităților publice la datele cu caracter personal în situații precum cea a transferului de date în cauză (și anume, în domeniul de reglementare specific; cu privire la tipul entităților din care face parte importatorul;...);
(3) să indice măsurile luate pentru a împiedica accesul la datele transferate (dacă este cazul);
(4) să furnizeze informații suficient de detaliate cu privire la toate cererile autorităților publice de accesare a datelor cu caracter personal primite de către importator într-o anumită perioadă,[77] în special în domeniile menționate la punctul (1) de mai sus și care cuprind informații privind cererile primite, datele solicitate, organismul solicitant și temeiul juridic pentru comunicare și în ce măsură importatorul a comunicat datele solicitate[78];
(5) să precizeze dacă și în ce măsură importatorului îi este interzis prin lege să furnizeze informațiile menționate la punctele (1)-(5) de mai sus.

101. Aceste informații ar putea fi furnizate prin intermediul unor chestionare structurate pe care importatorul le completează și semnează, însoțite de obligația contractuală a acestuia din urmă de a

[77] Durata perioadei ar trebui să depindă de riscul pentru drepturile și libertățile persoanelor vizate ale căror date fac obiectul transferului în cauză – de exemplu, ultimul an înainte de încheierea instrumentului de export de date cu exportatorul de date.
[78] Respectarea acestei obligații nu echivalează, în sine, cu asigurarea unui nivel de protecție adecvat. În același timp, orice comunicare necorespunzătoare care a avut loc efectiv conduce la necesitatea punerii în aplicare a unor măsuri suplimentare.

declara, într-un anumit termen, orice posibilă modificare a acestor informații, așa cum se procedează în prezent în cazul proceselor de diligență.

102. ***Condiții de eficacitate:***

- Importatorul trebuie să poată furniza exportatorului aceste tipuri de informații în deplină cunoștință de cauză și după ce a depus toate eforturile pentru a le obține[79].
- Această obligație impusă importatorului este un mijloc de a se asigura faptul că exportatorul este și rămâne conștient de riscurile asociate transferului de date către o țară terță. Astfel, aceasta va permite exportatorului să nu mai încheie contractul sau, în cazul în care informațiile se modifică după încheierea acestuia, să își îndeplinească obligația de a suspenda transferul și/sau de a rezilia contractul dacă legislația țării terțe, garanțiile cuprinse în instrumentul de transfer prevăzut la articolul 46 din RGPD utilizat și orice garanții suplimentare pe care le-ar fi putut adopta nu mai pot asigura un nivel de protecție în esență echivalent cu cel din UE. Însă, această obligație nu poate nici să justifice divulgarea de către importator a datelor cu caracter personal, nici să creeze așteptarea că nu vor mai exista cereri de acces.

***

103. ***De asemenea, exportatorul ar putea adăuga clauze prin care importatorul să certifice faptul că (1) nu a creat în mod intenționat uși secrete sau programe similare care ar putea fi utilizate pentru accesarea sistemului și/sau a datelor cu caracter personal (2) nu și-a conceput sau modificat în mod intenționat procesele comerciale într-un mod care să faciliteze accesul la sisteme sau date cu caracter personal și (3) că legislația națională sau politica guvernamentală nu impune importatorului să creeze sau să mențină uși secrete sau să faciliteze accesul la sisteme sau date cu caracter personal ori ca importatorul să dețină sau să predea cheia de criptare[80].***

104. ***Condiții de eficacitate:***

- Existența unei legislații sau a unor politici guvernamentale care să împiedice importatorii să divulge aceste informații ar putea face ineficace această clauză. Prin urmare, importatorul nu va putea să încheie contractul sau va trebui să notifice exportatorul cu privire la imposibilitatea sa de a-și respecta în continuare angajamentele contractuale[81].
- Contractul trebuie să includă sancțiuni și/sau posibilitatea exportatorului de a rezilia contractul într-un termen scurt în cazul în care importatorul nu dezvăluie existența unei uși secrete sau a unui program similar ori a unor procese comerciale manipulate sau a oricărei cereri de a le pune în aplicare sau nu informează exportatorul imediat după ce a luat cunoștință de existența acesteia.

***

[79] Vezi punctul 32.5 de mai sus.
[80] Această clauză este importantă pentru a garanta un nivel adecvat de protecție a datelor cu caracter personal transferate și, de obicei, ar trebui să fie obligatorie.
[81] Vezi punctul 32.5 de mai sus.

105. ***Exportatorul și-ar putea consolida competența de a efectua audituri[82] sau inspecții ale instalațiilor importatorului de prelucrare a datelor, la fața locului și/sau la distanță, pentru a verifica dacă datele au fost comunicate autorităților publice și în ce condiții (accesul nu depășește ceea ce este necesar și proporțional într-o societate democratică), de exemplu prin prevederea unui termen scurt și a unor mecanisme care să asigure intervenția rapidă a organismelor de control și prin consolidarea autonomiei exportatorului în ceea ce privește selectarea organismelor de control.***

106. ***Condiții de eficacitate:***

- Pentru a fi pe deplin eficace, domeniul de aplicare al auditului ar trebui să acopere, din punct de vedere juridic și tehnic, orice prelucrare de către persoanele împuternicite de operator sau subcontractanții importatorului a datelor cu caracter personal transmise în țara terță.
- Jurnalele de acces și alte jurnale similare ar trebui să fie inviolabile, astfel încât auditorii să poată găsi dovezi de divulgare. De asemenea, jurnalele de acces și alte jurnale similare ar trebui să facă distincția între accesul ca urmare a operațiunilor comerciale obișnuite și accesul ca urmare a unor ordine sau cereri de acces.

***

107. ***În cazul în care legislația și practica țării terțe a importatorului au fost evaluate inițial și s-a considerat că oferă un nivel de protecție în esență echivalent cu cel prevăzut în UE pentru datele transferate de către exportator, acesta din urmă ar putea totuși să consolideze obligația importatorului de date de a informa imediat exportatorul de date cu privire la imposibilitatea sa de a respecta angajamentele contractuale și, prin urmare, standardul necesar de „nivel de protecție a datelor în esență echivalent”[83].***

108. Această imposibilitate de a se conforma poate rezulta din modificările legislației sau ale practicii țării terțe[84]. Clauzele ar putea stabili termene și proceduri specifice și stricte pentru suspendarea rapidă a transferului de date și/sau rezilierea contractului și returnarea sau ștergerea de către importator a datelor primite. Urmărirea cererilor primite, a domeniului de aplicare al acestora și a eficacității măsurilor adoptate pentru a le contracara ar trebui să ofere exportatorului suficiente informații pentru a-și exercita obligația de a suspenda sau de a înceta transferul și/sau de a rezilia contractul.

109. ***Condiții de eficacitate:***

- Notificarea trebuie să aibă loc înainte să fie acordat accesul la date. În caz contrar, până la momentul primirii notificării de către exportator, este posibil ca drepturile persoanei să fi fost deja încălcate dacă cererea se bazează pe legislația țării terțe care depășește nivelul de protecție a datelor prevăzut de legislația UE. Notificarea poate totuși împiedica încălcările

[82] Vezi, de exemplu, clauza 5 litera (f) din Decizia 2010/87/UE privind CCS între operatori și persoanele împuternicite de operatori, auditurile ar putea fi, de asemenea, prevăzute în cadrul unui cod de conduită sau prin certificare.

[83] Clauza 5 litera (a) și litera (d) punctul (i) din Decizia 2010/87/UE privind CCS.

[84] Vezi cauza C-311/18 (Schrems II), punctul 139, în care Curtea afirmă că *„deși clauza 5 litera (d) punctul (i) permite destinatarului transferului de date cu caracter personal să nu notifice operatorului stabilit în Uniune o solicitare, obligatorie din punct de vedere juridic, de a divulga date cu caracter personal, prezentată de o autoritate de aplicare a legii, în cazul unei legislații care îi interzice acest lucru, precum interdicția, în cadrul dreptului penal, de a păstra confidențialitatea unei investigații urmărind aplicarea legii, acesta este totuși obligat, în conformitate cu clauza 5 litera (a) din anexa la Decizia Clauzele standard, să informeze operatorul cu privire la imposibilitatea sa de a asigura conformitatea cu clauzele standard de protecție a datelor”*.

viitoare și permite exportatorului să își îndeplinească obligația de a suspenda transferul de date cu caracter personal către țara terță și/sau de a rezilia contractul.

- Importatorul de date trebuie să monitorizeze orice evoluții juridice sau politice care l-ar putea pune în imposibilitatea de a-și respecta obligațiile și trebuie să informeze imediat exportatorul de date cu privire la orice astfel de modificări și evoluții și, dacă este posibil, înainte de punerea acestora în aplicare, pentru a-i permite exportatorului de date să recupereze datele de la importatorul de date.
- Clauzele ar trebui să prevadă un mecanism rapid prin care exportatorul de date să autorizeze importatorul de date să securizeze datele sau să le returneze imediat exportatorului de date sau, dacă acest lucru nu este fezabil, să șteargă sau să cripteze în siguranță datele, fără a aștepta neapărat instrucțiunile exportatorului, dacă se atinge un anumit prag care urmează să fie convenit între exportatorul de date și importatorul de date. Importatorul ar trebui să pună în aplicare acest mecanism de la începutul transferului de date și să îl testeze periodic pentru a se asigura că acesta poate fi aplicat într-un termen scurt.
- Alte clauze ar putea permite exportatorului să monitorizeze prin audituri, inspecții și alte măsuri de verificare îndeplinirea de către importator a acestor obligații și să asigure respectarea acestora, cu sancțiuni pentru importator și/sau cu posibilitatea exportatorului de a suspenda transferul și/sau de a rezilia imediat contractul.

***

110. ***În măsura în care legislația națională din țara terță permite acest lucru, contractul ar putea consolida obligațiile de transparență ale importatorului prin prevederea unei metode „Warrant Canary", prin care importatorul se angajează să publice periodic (de exemplu, cel puțin o dată la 24 de ore) un mesaj semnat criptografic prin care să informeze exportatorul că, de la o anumită dată și oră, nu a primit niciun ordin de comunicare a datelor cu caracter personal sau a altor informații similare. Lipsa unei actualizări a acestei notificări îi va indica exportatorului faptul că este posibil ca importatorul să fi primit un ordin.***

111. ***Condiții de eficacitate:***

- Reglementările țării terțe trebuie să permită importatorului de date să emită exportatorului această formă de notificare pasivă.
- Exportatorul de date trebuie să monitorizeze automat notificările „Warrant Canary".
- Importatorul de date trebuie să se asigure că cheia sa privată pentru semnarea „Warrant Canary" este păstrată în siguranță și că reglementările țării terțe nu îl pot obliga să emită notificări „Warrant Canary" false. În acest scop, ar putea fi util dacă mai multe semnături ar fi necesare din partea unor persoane diferite și/sau dacă „Warrant Canary" ar fi emis de o persoană din afara jurisdicției țării terțe.

Obligații de a lua măsuri specifice

112. ***Importatorul s-ar putea angaja să revizuiască, în temeiul legislației țării de destinație, legalitatea oricărui ordin de comunicare a datelor, în special dacă acesta rămâne în sfera de competență acordată autorității publice solicitante, și să conteste ordinul în cazul în care, în urma unei evaluări atente, ajunge la concluzia că există motive, în temeiul legislației țării de destinație, de a face acest lucru. Atunci când contestă un ordin, importatorul de date ar trebui să solicite acordarea unor măsuri***

provizorii de suspendare a efectelor ordinului până când instanța se pronunță pe fond. Importatorul ar avea obligația de a nu comunica datele cu caracter personal solicitate până când nu este obligat să o facă, în temeiul normelor procedurale aplicabile. Importatorul de date s-ar angaja, de asemenea, să furnizeze volumul minim de informații permis atunci când răspunde la ordin, în temeiul unei interpretări rezonabile a ordinului.

113. ***Condiții de eficacitate:***

- Ordinea juridică a țării terțe trebuie să ofere căi legale eficiente de contestare a ordinelor de comunicare a datelor.
- Această clauză va oferi întotdeauna o protecție suplimentară foarte limitată, deoarece un ordin de comunicare a datelor poate fi legal în temeiul ordinii juridice a țării terțe, dar este posibil ca această ordine juridică să nu respecte standardele UE. Această măsură contractuală va trebui să fie, în mod obligatoriu, complementară altor măsuri suplimentare.
- Contestarea ordinelor trebuie să aibă un efect suspensiv în temeiul legislației țării terțe. În caz contrar, autoritățile publice ar avea în continuare acces la datele persoanelor, iar orice acțiune subsecventă în favoarea persoanei ar limita efectul admiterii acțiunii în despăgubiri pentru consecințele negative care decurg din comunicarea datelor.
- Importatorul va trebui să poată documenta și demonstra exportatorului măsurile pe care le-a întreprins, depunând toate eforturile pentru a îndeplini acest angajament.

***

114. ***În aceeași situație descrisă mai sus, importatorul s-ar putea angaja să informeze autoritatea publică solicitantă cu privire la incompatibilitatea ordinului cu garanțiile cuprinse în instrumentul de transfer prevăzut la articolul 46 din RGPD[85] și cu privire la conflictul de obligații care rezultă pentru importator. Importatorul ar notifica simultan și cât mai curând posibil exportatorul și/sau autoritatea de supraveghere competentă din SEE, în măsura în care acest lucru este posibil în temeiul ordinii juridice a țării terțe.***

115. ***Condiții de eficacitate:***

- Astfel de informații privind protecția conferită de dreptul Uniunii și conflictul de obligații ar trebui să aibă anumite efecte juridice în ordinea juridică a țării terțe, cum ar fi un control judiciar sau administrativ al ordinului sau al cererii de acces, obligativitatea obținerii unui mandat judiciar și/sau o suspendare temporară a ordinului de a adăuga o anumită protecție datelor.
- Sistemul juridic al țării nu trebuie să împiedice importatorul să notifice exportatorul sau cel puțin autoritatea de supraveghere competentă din SEE cu privire la ordinul sau cererea de acces primită.

[85] De exemplu, CCS prevăd că prelucrarea datelor, inclusiv transferul acestora, a fost și va continua să fie efectuată în conformitate cu *„legea aplicabilă privind protecția datelor”.* Această lege este definită ca *„legislația care protejează drepturile și libertățile fundamentale ale particularilor și, în special, dreptul lor la viață privată cu privire la prelucrarea datelor cu caracter personal, aplicabilă operatorului de date din statul membru în care este stabilit exportatorul de date”.* CJUE confirmă că dispozițiile RGPD, interpretate în lumina Cartei drepturilor fundamentale a Uniunii Europene, fac parte din legislația respectivă; vezi CJUE C-311/18 (Schrems II), punctul 138.

- Importatorul va trebui să poată documenta și demonstra exportatorului măsurile pe care le-a întreprins, depunând toate eforturile pentru a îndeplini acest angajament.

Împuternicirea persoanelor vizate de a-și exercita drepturile

116. ***Contractul ar putea prevedea ca datele cu caracter personal transmise sub formă de text simplu în cursul normal al activității (inclusiv în situații de acordare de asistență) să poată fi accesate numai cu consimțământul explicit sau implicit al exportatorului și/sau al persoanei vizate.***

117. ***Condiții de eficacitate:***

- Această clauză ar putea fi eficace în situațiile în care importatorii primesc cereri din partea autorităților publice de cooperare voluntară, spre deosebire, de exemplu, de accesul autorităților publice la date, care are loc fără cunoștința importatorului de date sau împotriva voinței acestuia.
- În unele situații, este posibil ca persoana vizată să nu fie în măsură să se opună accesului sau să își dea consimțământul care îndeplinește toate condițiile prevăzute de legislația UE (liber exprimat, specific, informat și lipsit de ambiguitate) (de exemplu, în cazul angajaților)[86].
- Reglementările sau politicile naționale care obligă importatorul să nu comunice ordinul de acces pot anula eficacitatea acestei clauze, cu excepția cazului în care poate fi susținută prin metode tehnice care necesită intervenția exportatorului sau a persoanei vizate pentru ca datele din textul simplu să fie accesibile. Astfel de măsuri tehnice de restricționare a accesului pot fi avute în vedere în special dacă accesul este acordat numai în cazuri specifice de asistență sau de service, dar datele propriu-zise sunt stocate în cadrul SEE.

***

118. ***Contractul ar putea obliga importatorul și/sau exportatorul să notifice imediat persoana vizată cu privire la cererea sau ordinul primit de la autoritățile publice din țara terță sau cu privire la imposibilitatea importatorului de a-și respecta angajamentele contractuale, pentru a permite persoanei vizate să solicite informații și să recurgă la o cale de atac eficientă (de exemplu, prin depunerea unei plângeri la autoritatea sa de supraveghere competentă și/sau la autoritatea judiciară pentru a-și demonstra calitate procesuală activă în fața instanțelor din țara terță).***

119. ***Condiții de eficacitate:***

- Această notificare ar putea avertiza persoana vizată cu privire la posibila accesare a datelor sale de către autoritățile publice din țările terțe. Astfel, aceasta ar putea permite persoanei vizate să solicite informații suplimentare de la exportatori și să depună o plângere la autoritatea sa de supraveghere competentă. Această clauză ar putea aborda, de asemenea, unele dintre dificultățile cu care se poate confrunta o persoană în ceea ce privește demonstrarea calității sale procesuale active *(locus standi)* în fața instanțelor din țări terțe, pentru a contesta accesul autorităților publice la datele sale.
- Reglementările și politicile naționale pot împiedica notificarea persoanei vizate. Cu toate acestea, exportatorul și importatorul s-ar putea angaja să informeze persoana vizată de îndată ce restricțiile privind comunicarea datelor sunt eliminate și să depună toate eforturile pentru

[86] Vezi articolul 4 alineatul (11) din RGPD.

a obține derogarea de la interdicția de comunicare. Exportatorul sau autoritatea de supraveghere competentă ar putea notifica persoana vizată cel puțin cu privire la suspendarea sau încetarea transferului datelor sale cu caracter personal din cauza imposibilității importatorului de a-și respecta angajamentele contractuale ca urmare a primirii unei cereri de acces.

***

120. ***Contractul ar putea obliga exportatorul și importatorul să acorde asistență persoanei vizate în ceea ce privește exercitarea drepturilor sale în jurisdicția țării terțe prin mecanisme de atac ad-hoc și consiliere juridică.***

121. ***Condiții de eficacitate***

- Reglementările și politicile naționale pot impune condiții care pot submina eficacitatea mecanismelor de atac ad-hoc prevăzute.
- Consilierea juridică ar putea fi utilă pentru persoana vizată, în special având în vedere cât de complicat și de costisitor poate fi ca o persoană vizată să înțeleagă sistemul juridic al unei țări terțe și să introducă acțiuni în justiție din străinătate, eventual într-o limbă străină. Cu toate acestea, această clauză va oferi întotdeauna o protecție suplimentară limitată, deoarece acordarea de asistență și consiliere juridică persoanelor vizate nu poate compensa lipsa prevederii în ordinea juridică a unei țări terțe a unui nivel de protecție în esență echivalent cu cel garantat în cadrul UE. Această măsură contractuală va trebui să fie, în mod obligatoriu, complementară altor măsuri suplimentare.

Această măsură suplimentară ar fi eficace numai cu condiția ca legislația țării terțe să prevadă căi de atac în fața instanțelor sale naționale sau să existe un mecanism de atac ad-hoc. În orice caz, aceasta nu ar fi însă o măsură suplimentară eficientă împotriva măsurilor de supraveghere în cazul în care nu există niciun mecanism de atac.

Măsuri organizatorice

122. Măsurile organizatorice suplimentare pot consta în politici interne, metode organizatorice și standarde pe care operatorii și persoanele împuternicite de operatori le-ar putea aplica lor înșelor și importatorilor de date din țări terțe. Acestea pot contribui la asigurarea coerenței în ceea ce privește protecția datelor cu caracter personal pe parcursul întregului ciclu de prelucrare. Măsurile organizatorice pot îmbunătăți, de asemenea, gradul de conștientizare a exportatorilor cu privire la riscurile și încercările de a obține acces la date în țări terțe, precum și la capacitatea lor de a reacționa la acestea. Selectarea și punerea în aplicare a uneia sau a mai multora dintre aceste măsuri nu vor garanta în mod obligatoriu și sistematic faptul că transferul dumneavoastră îndeplinește standardul de echivalență esențială impus de dreptul UE. În funcție de circumstanțele specifice ale transferului și de evaluarea efectuată cu privire la legislația țării terțe, sunt necesare măsuri organizatorice pentru a completa măsurile contractuale și/sau tehnice, în vederea asigurării unui nivel de protecție a datelor cu caracter personal în esență echivalent cu cel garantat în cadrul UE.

123. Evaluarea celor mai adecvate măsuri trebuie efectuată de la caz la caz, ținând seama de necesitatea ca operatorii și persoanele împuternicite de operatori să respecte principiul responsabilității. În continuare, CEPD enumeră câteva exemple de măsuri organizatorice pe care exportatorii le pot pune în aplicare, cu toate că lista nu este exhaustivă și pot fi, de asemenea, adecvate alte măsuri:

Politici interne de guvernanță a transferurilor, în special între grupuri de întreprinderi

124. ***Adoptarea unor politici interne adecvate, cu alocarea clară a responsabilităților pentru transferurile de date, a canalelor de raportare și a procedurilor standard de operare în cazurile de cereri disimulate sau oficiale din partea autorităților publice de a avea acces la date. În special în cazul transferurilor între grupuri de întreprinderi, aceste politici pot include, printre altele, numirea unei echipe specifice, care ar trebui să aibă sediul în cadrul SEE, compusă din experți în domeniul legislației privind tehnologia informațiilor, protecția datelor și confidențialitatea, care să se ocupe de cererile ce implică date cu caracter personal transferate din UE; notificarea structurilor juridice și corporative superioare și a exportatorului de date la primirea unor astfel de cereri; etapele procedurale pentru contestarea cererilor disproporționate sau ilegale și furnizarea de informații transparente persoanelor vizate.***

125. Elaborarea unor proceduri specifice de formare pentru personalul responsabil cu gestionarea cererilor autorităților publice de acces la datele cu caracter personal, proceduri care ar trebui actualizate periodic pentru a reflecta noile evoluții legislative și jurisprudențiale din țara terță și din SEE. Procedurile de formare ar trebui să includă cerințele dreptului Uniunii privind accesul autorităților publice la datele cu caracter personal, în special astfel cum rezultă din articolul 52 alineatul (1) din Carta drepturilor fundamentale. Ar trebui să fie sporită conștientizarea personalului în special prin evaluarea exemplelor practice ale cererilor autorităților publice de acces la date și prin aplicarea standardului care decurge din articolul 52 alineatul (1) din Carta drepturilor fundamentale unor astfel de exemple practice. O astfel de formare ar trebui să țină seama de situația specială a importatorului de date, de exemplu legislația și reglementările țării terțe care i se aplică importatorului de date, și ar trebui dezvoltată, acolo unde este posibil, în cooperare cu exportatorul de date.

126. ***Condiții de eficacitate:***

- Aceste politici pot fi avute în vedere numai în cazul în care cererea autorităților publice din țara terță este compatibilă cu dreptul Uniunii[87]. În cazul în care cererea este incompatibilă, aceste politici nu ar fi suficiente pentru a asigura un nivel echivalent de protecție a datelor cu caracter personal și, astfel cum s-a menționat anterior, transferurile trebuie oprite sau trebuie puse în aplicare măsuri suplimentare adecvate pentru a evita accesul la date.

Măsuri de transparență și responsabilitate

127. ***Documentează și înregistrează cererile de acces primite de la autoritățile publice și răspunsul oferit, împreună cu raționamentul juridic și actorii implicați (de exemplu, dacă exportatorul a fost notificat și răspunsul acestuia, evaluarea echipei care se ocupă de aceste cereri etc.). Aceste evidențe ar trebui să fie puse la dispoziția exportatorului de date, care, la rândul său, ar trebui să le furnizeze persoanelor vizate, dacă este necesar.***

128. ***Condiții de eficacitate:***

- Legislația națională a țării terțe poate împiedica comunicarea cererilor sau a unor informații substanțiale cu privire la acestea și, prin urmare, poate anula eficacitatea acestei practici. Importatorul de date ar trebui să informeze exportatorul cu privire la imposibilitatea sa de a furniza astfel de documente și evidențe, oferindu-i astfel exportatorului opțiunea de a

[87] Vezi cauza C-362/14 („Schrems I”), punctul 94; C-311/18 (Schrems II), punctele 168, 174, 175 și 176.

suspenda transferurile în cazul în care o astfel de imposibilitate ar conduce la o scădere a nivelului de protecție.

***

129. ***Publicarea periodică de rapoarte de transparență sau rezumate cu privire la cererile guvernamentale de acces la date și tipul de răspuns furnizat, în măsura în care publicarea este permisă de legislația locală.***

130. ***Condiții de eficacitate:***

- Informațiile furnizate ar trebui să fie relevante, clare și cât mai detaliate posibil. Legislația națională a țării terțe poate împiedica comunicarea de informații detaliate. În aceste cazuri, importatorul de date ar trebui să depună toate eforturile pentru a publica informații statistice sau tipuri de informații agregate similare.

Metode organizatorice și măsuri de reducere la minimum a datelor

131. ***Cerințele organizatorice deja existente în temeiul principiului responsabilității, cum ar fi adoptarea unor și politici și bune practici stricte și detaliate privind accesul la date și confidențialitatea, bazate pe principiului strict al necesității de a cunoaște, monitorizate prin audituri periodice și puse în aplicare prin măsuri disciplinare pot fi, de asemenea, măsuri utile în contextul transferului. În acest sens, ar trebui avută în vedere reducerea la minimum a datelor, pentru a limita expunerea datelor cu caracter personal la accesul neautorizat. De exemplu, în unele cazuri, s-ar putea ca transferul anumitor date să nu fie necesar (de exemplu, în cazul accesului de la distanță la datele SEE, cum ar fi în cazul acordării de asistență, atunci când se acordă acces restricționat în loc de acces deplin sau atunci când, pentru a furniza un serviciu, este nevoie doar de transferul unui set limitat de date, și nu al unei baze de date complete).***

132. ***Condiții de eficacitate:***

- Ar trebui să existe audituri periodice și măsuri disciplinare ferme pentru a monitoriza și a asigura respectarea măsurilor de reducere la minimum a datelor și în contextul transferului.
- Exportatorul de date efectuează o evaluare a datelor cu caracter personal aflate în posesia sa, înainte ca transferul să aibă loc, pentru a identifica seturile de date care nu sunt necesare în scopul transferului și, prin urmare, care nu vor fi comunicate importatorului de date.
- Măsurile de reducere la minimum a datelor ar trebui să fie însoțite de măsuri tehnice, pentru a se asigura că datele nu fac obiectul accesului neautorizat. De exemplu, punerea în aplicare a unor mecanisme de calcul multipartit securizat și distribuirea seturilor de date criptate între diferite entități de încredere pot împiedica, în mod intrinsec, comunicarea de date identificabile ca urmare a oricărui acces unilateral.

***

133. ***Elaborarea unor bune practici pentru a implica în mod adecvat și în timp util responsabilul cu protecția datelor, dacă acesta există, precum și serviciile juridice și de audit intern și a le oferi acces la informații cu privire la aspectele legate de transferurile internaționale de date cu caracter personal.***

134. ***Condiții de eficacitate:***

- Responsabilul cu protecția datelor, dacă acesta există, și echipa juridică și de audit intern primesc toate informațiile relevante înainte de transfer și sunt consultate cu privire la necesitatea transferului și la garanțiile suplimentare, dacă este cazul.
- Informațiile relevante ar trebui să includă, de exemplu, evaluarea necesității transferului anumitor date cu caracter personal, o prezentare generală a legislației aplicabile a țării terțe și garanțiile pe care importatorul s-a angajat să le pună în aplicare.

Adoptarea standardelor și a bunelor practici

135. ***Adoptarea unor politici stricte privind securitatea și confidențialitatea datelor, pe baza certificării UE sau a codurilor de conduită ori a standardelor internaționale (de exemplu, normele ISO) și a bunelor practici (de exemplu, ENISA), ținând seama în mod corespunzător de stadiul actual al tehnologiei, în conformitate cu riscul categoriilor de date prelucrate și cu probabilitatea încercărilor autorităților publice de a obține acces la acestea.***

Altele

136. ***Adoptarea și revizuirea periodică a politicilor interne pentru a evalua caracterul adecvat al măsurilor complementare puse în aplicare și pentru a identifica și a pune în aplicare soluții suplimentare sau alternative atunci când este necesar, în scopul asigurării menținerii unui nivel de protecție echivalent cu cel garantat în cadrul UE pentru datele cu caracter personal transferate.***

***

137. ***Angajamentele importatorului de date de a nu se angaja în niciun transfer ulterior al datelor cu caracter personal în aceeași țară terță sau în alte țări terțe sau de a suspenda transferurile în curs, atunci când în țara terță nu se poate asigura un nivel de protecție a datelor cu caracter personal echivalent cu cel garantat în cadrul UE[88].***

[88] C-311/18 (Schrems II), punctele 135 și 137.

ANEXA 3: POSIBILE SURSE DE INFORMAȚII PENTRU EVALUAREA UNEI ȚĂRI TERȚE

138. Importatorul dumneavoastră de date ar trebui să fie în măsură să vă pună la dispoziție surse și informații relevante cu privire la țara terță în care este stabilit și la legislația aplicabilă. De asemenea, puteți face trimitere la mai multe surse de informații, cum ar fi cele enumerate mai jos, în mod neexhaustiv:

- Jurisprudența Curții de Justiție a Uniunii Europene (CJUE) și a Curții Europene a Drepturilor Omului (CEDO)[89], astfel cum este menționată în recomandările privind garanțiile esențiale europene[90];
- Deciziile privind caracterul adecvat al nivelului de protecție în țara de destinație, în cazul în care transferul se bazează pe un temei juridic diferit[91];
- Rezoluții și rapoarte din partea organizațiilor interguvernamentale, cum ar fi Consiliul Europei,[92] alte organisme regionale[93] și organisme și agenții ONU (de exemplu, Consiliul pentru Drepturile Omului,[94] Comitetul pentru Drepturile Omului[95]);
- Jurisprudența națională sau deciziile luate de autoritățile judiciare sau administrative independente competente în domeniul confidențialității și protecției datelor din țările terțe;
- Rapoarte ale instituțiilor academice și ale organizațiilor societății civile (de exemplu, ONG-uri și asociații profesionale).

[89] Vezi fișa informativă a jurisprudenței CEDO privind supravegherea în masă: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

[90] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

[91] C-311/18 (Schrems II), punctul 141; vezi deciziile privind caracterul adecvat al nivelului de protecție din https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_ro

[92] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

[93] Vezi, de exemplu, rapoartele de țară ale Comisiei Interamericane a Drepturilor Omului (IACHR), https://www.oas.org/en/iachr/reports/country.asp.

[94] Vezi https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx

[95] vezi: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5