Avizul 22/2024 privind anumite obligații care decurg din folosirea persoanei (persoanelor) împuternicite de operator și a subcontractantului (subcontractanților)

Adoptat la 7 octombrie 2024

Rezumat

AS daneză a solicitat CEPD să emită un aviz cu privire la chestiuni de aplicare generală în conformitate cu articolul 64 alineatul (2) din RGPD. Avizul contribuie la interpretarea armonizată de către autoritățile naționale de supraveghere a anumitor aspecte ale articolului 28 din RGPD, după caz în coroborare cu capitolul V din RGPD. În particular, avizul abordează chestiuni referitoare la interpretarea anumitor obligații ale operatorilor care se bazează pe persoanele împuternicite de operatori și pe subcontractanți, care decurg în special din articolul 28 din RGPD, precum și din formularea contractelor dintre operator și persoana împuternicită de operator. Întrebările vizează prelucrarea datelor cu caracter personal în SEE, precum și prelucrarea în urma unui transfer către o țară terță.

Comitetul concluzionează în acest aviz că operatorii trebuie să aibă acces rapid și în orice moment la informațiile privind identitatea (și anume numele, adresa, persoana de contact) tuturor persoanelor împuternicite de operatori, a subcontractanților etc., astfel încât să-și poată îndeplini cel mai bine obligațiile care le revin în temeiul articolului 28 din RGPD, indiferent de riscul asociat activității de prelucrare. În acest scop, persoana împuternicită de operator trebuie să furnizeze în mod proactiv operatorului toate aceste informații și trebuie să le actualizeze permanent.

Articolul 28 alineatul (1) din RGPD prevede că operatorii au obligația să recurgă la persoane împuternicite care oferă „garanții suficiente" pentru a pune în aplicare măsuri „adecvate" astfel încât prelucrarea să respecte cerințele RGPD și să asigure protecția drepturilor persoanelor vizate. CEPD consideră, în avizul său, că, atunci când evaluează respectarea de către operatori a acestei obligații și a principiului responsabilității [articolul 24 alineatul (1) din RGPD], autoritățile de supraveghere ar trebui să considere că implicarea persoanelor împuternicite de operatori nu trebuie să reducă nivelul de protecție a drepturilor persoanelor vizate. *Obligația* operatorului de a verifica dacă persoanele împuternicite de operator (subcontractanții) prezintă „garanții suficiente" pentru a pune în aplicare măsurile adecvate stabilite de operator ar trebui să se aplice indiferent de riscul pentru drepturile și libertățile persoanelor vizate. *Amploarea* acestei verificări va varia însă în practică în funcție de natura acestor măsuri tehnice și organizatorice, care pot fi mai stricte sau mai extinse în funcție de nivelul unui astfel de risc.

CEPD precizează, de asemenea, în aviz că, deși persoana împuternicită inițială trebuie să se asigure că propune subcontractanți care oferă garanții suficiente, decizia finală privind recurgerea la un anumit subcontractant și responsabilitatea aferentă, inclusiv în ceea ce privește verificarea garanțiilor, revine operatorului. AS trebuie să evalueze dacă operatorul este în măsură să demonstreze că verificarea suficienței garanțiilor furnizate de persoanele împuternicite de operator (subcontractanți) a avut loc în mod satisfăcător pentru operator. Operatorul poate alege să se bazeze pe informațiile primite de la persoana împuternicită de operator și să le dezvolte dacă este nevoie (de exemplu, când par incomplete, inexacte sau ridică semne de întrebare). Mai precis, pentru prelucrarea care prezintă un risc mare pentru drepturile și libertățile persoanelor vizate, operatorul trebuie să-și sporească nivelul de verificare în ceea ce privește verificarea informațiilor furnizate. În această privință, CEPD consideră că, în conformitate cu RGPD, operatorul nu are obligația de a solicita sistematic contractele de subcontractare pentru a controla dacă obligațiile de protecție a datelor prevăzute în contractul inițial au fost transmise de-a lungul lanțului de prelucrare. Operatorul trebuie să evalueze, de la caz la caz,

dacă solicitarea unei copii a acestor contracte sau revizuirea lor în orice moment este necesară pentru a putea demonstra conformitatea în lumina principiului responsabilității.

În cazul în care transferurile de date cu caracter personal în afara SEE au loc între două persoane împuternicite de operator (subcontractanți), în conformitate cu instrucțiunile operatorului, operatorul este în continuare supus obligațiilor care decurg din articolul 28 alineatul (1) din RGPD privind „garanțiile suficiente", pe lângă cele prevăzute la articolul 44, pentru a se asigura că nivelul de protecție garantat de RGPD nu este subminat de transferurile de date cu caracter personal. Persoana împuternicită de operator/exportatorul trebuie să pregătească documentația relevantă, în conformitate cu jurisprudența și după cum se explică în Recomandările CEPD nr. 1/2020. Operatorul trebuie să evalueze și să fie în măsură să prezinte autorității de supraveghere competente această documentație. Operatorul se poate baza pe documentația sau informațiile primite de la persoana împuternicită de operator/exportator și, dacă este nevoie, le poate dezvolta. Amploarea și natura obligației operatorului de a evalua această documentație pot depinde de motivul utilizat pentru transfer și dacă transferul constituie un transfer inițial sau ulterior.

CEPD a abordat, de asemenea, în aviz, o chestiune referitoare la formularea contractelor dintre operator și persoana împuternicită de operator. În acest sens, un element de bază este angajamentul persoanei împuternicite de operator de a prelucra datele cu caracter personal numai pe baza unor instrucțiuni documentate din partea operatorului, cu excepția cazului în care persoana împuternicită de operator este obligată să [prelucreze] datele *„în temeiul dreptului Uniunii sau al dreptului intern care i se aplică*" [articolul 28 alineatul (3) litera (a) din RGPD] - reamintind principiul general conform căruia contractele nu pot prevala asupra legii. Având în vedere libertatea contractuală acordată părților pentru a-și adapta contractul operator-persoană împuternicită de operator la propriile circumstanțe, în limitele articolului 28 alineatul (3) din RGPD, CEPD este de părere că includerea cuvintelor „*cu excepția cazului în care persoanei împuternicite de operator îi revine această obligație în temeiul dreptului Uniunii sau al dreptului intern care i se aplică*" (textual sau în termeni foarte similari) este foarte recomandată, dar nu obligatorie.

În ceea ce privește variantele similare cu „*cu excepția cazului în care obligația îi revine în temeiul dreptului sau al unei ordonanțe obligatorii al unui organism guvernamental* ", CEPD consideră că acest lucru rămâne în prerogativa libertății contractuale a părților și nu încalcă articolul 28 alineatul (3) litera (a) din RGPD per se. În același timp, CEPD identifică în avizul său o serie de probleme, deoarece o asemenea clauză nu exonerează persoana împuternicită de operator de respectarea obligațiilor care îi revin în temeiul RGPD.

Pentru datele cu caracter personal transferate în afara SEE, CEPD consideră că este puțin probabil ca formularea „*cu excepția cazului în care obligația îi revine în temeiul legii sau al unei ordonanțe obligatorii a unui organism guvernamental*" să fie suficientă, în sine, pentru a asigura conformitatea cu articolul 28 alineatul (3) litera (a) din RGPD, coroborat cu capitolul V. După cum reiese din CCS-urile Comisiei Europene privind transferul internațional și din recomandările RCO-O, articolul 28 alineatul (3) litera (a) din RGPD nu împiedică - în principiu - includerea în contract a unor dispoziții care abordează cerințele legislației unei țări terțe în ceea ce privește prelucrarea datelor cu caracter personal transferate. Cu toate acestea, ca și în aceste documente, trebuie făcută distincția între legislația (legile) țării (țărilor) terțe care ar submina nivelul de protecție garantat de RGPD și cele care nu ar face acest lucru. În fine, CEPD reamintește că posibilitatea ca legislația unei țări terțe să împiedice

respectarea RGPD ar trebui să fie un factor luat în considerare de părți înainte de încheierea contractului (între operator și persoana împuternicită de operator sau între persoana împuternicită de operator și subcontractant).

În cazul în care persoana împuternicită de operator prelucrează date cu caracter personal în cadrul SEE, aceasta se poate confrunta în continuare cu legislația țărilor terțe, în anumite circumstanțe. CEPD subliniază că adăugarea în contract a unei formulări similare cu *„cu excepția cazului în care această obligație îi revine în temeiul legii sau al unei ordonanțe obligatorii a unui organism guvernamental”* nu exonerează persoana împuternicită de operator de obligațiile care îi revin în temeiul RGPD.

În cele din urmă, CEPD este de părere că monitorizarea angajamentului persoanei împuternicite de operator de a prelucra numai instrucțiuni documentate cu *„cu excepția cazului în care această obligație îi revine în temeiul legii sau al unei ordonanțe obligatorii a unui organism guvernamental*” (textual sau în termeni foarte similari) nu poate fi interpretată ca instrucțiune documentată a operatorului.

Cuprins

1 Introducere 6

1.1 Expunerea sumară a faptelor 6

1.2 Admisibilitatea cererii de emitere a unui aviz în temeiul articolului 64 alineatul (2) din RGPD 8

2 Cu privire la temeinicia cererii 9

2.1 Cu privire la interpretarea articolului 28 alineatul (1), a articolului 28 alineatul (2) și a articolului 28 alineatul (4) din RGPD coroborate cu articolul 5 alineatul (2) și cu articolul 24 alineatul (1) (întrebările 1.1 și 1.3) 9

2.1.1 Identificarea actorilor din lanțul de prelucrare 10

2.1.2 Verificarea și documentarea de către operator a suficienței garanțiilor oferite de toate persoanele împuternicite de operator din lanțul de prelucrare 13

2.1.3 Verificarea contractului dintre persoana împuternicită inițială și persoanele împuternicite suplimentare 19

2.2 Cu privire la interpretarea articolului 28 alineatul (1) din RGPD coroborat cu articolul 44 din RGPD (transferuri în lanțul de prelucrare - întrebările 1.2 și 1.3) 23

2.3 Cu privire la interpretarea articolului 28 alineatul (3) litera (a) din RGPD (întrebarea 2) 30

Comitetul european pentru protecția datelor

Având în vedere articolul 63 și articolul 64 alineatul (2) 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 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 10 și 22 din Regulamentul său de procedură,

întrucât:

(1) Principalul rol al Comitetului European pentru Protecția Datelor (denumit în continuare „CEPD”) este de a asigura aplicarea coerentă a RGPD în întregul Spațiu Economic European („SEE”). Articolul 64 alineatul (2) din RGPD prevede că orice autoritate de supraveghere (AS), președintele Comitetului sau Comisia poate solicita ca orice chestiune de aplicare generală sau care produce efecte în mai mult de un stat membru SEE să fie examinată de Comitet în vederea obținerii unui aviz. Scopul acestui aviz este de a analiza o chestiune de aplicare generală sau care produce efecte în mai mult de un stat membru SEE.

(2) Avizul Comitetului se adoptă în temeiul articolului 64 alineatul (3) din RGPD, coroborat cu articolul 10 alineatul (2) din Regulamentul de procedură al Comitetului European pentru Protecția Datelor, în termen de opt săptămâni de la prima zi lucrătoare după ce președintele și autoritatea de supraveghere competentă decid că dosarul este complet. Prin decizia președintelui, această perioadă poate fi prelungită cu șase săptămâni, în funcție de complexitatea chestiunii.

ADOPTĂ URMĂTORUL AVIZ:

1 INTRODUCERE

1.1 Expunerea sumară a faptelor

1. La 5 iulie 2024, Autoritatea daneză de supraveghere (denumită în continuare „AS DK”) a cerut Comitetului European pentru Protecția Datelor (denumit în continuare „CEPD” sau „Comitetul”) să emită un aviz cu privire la obligațiile responsabilității operatorilor în ceea ce privește lanțul de prelucrare și relația dintre operatori și persoanele împuternicite de operatori (subcontractanți) (denumită în continuare „cererea”).

2. AS DK a declarat dosarul complet la 8 iulie 2024. Președintele Comitetului a considerat dosarul complet la 9 iulie 2024. La aceeași dată, dosarul a fost difuzat de Secretariatul CEPD. Președintele, având în

[1] Trimiterile la „statele membre” din acest aviz trebuie înțelese ca trimiteri la „statele membre ale SEE”. Trimiterile la „Uniune” din prezentul aviz trebuie înțelese ca trimiteri la „SEE”.

vedere complexitatea problemei, a decis să prelungească termenul legal în conformitate cu articolul 64 alineatul (3) din RGPD și cu articolul 10 alineatul (4) din Regulamentul de procedură.

3. AS DK se referă în cererea sa și la raportul adoptat de CEPD în ianuarie 2023 privind constatările primei sale acțiuni coordonate de punere în aplicare[2] în cadrul Cadrului coordonat de punere în aplicare (CEF)[3]. Această acțiune coordonată s-a axat pe utilizarea de către sectorul public a serviciilor bazate pe cloud. În raportul CEPD, autoritățile de supraveghere care au participat la acțiunea coordonată au identificat opt provocări, în special în ceea ce privește utilizarea de către organismele publice a serviciilor de cloud, și au furnizat o listă de puncte de interes pe care părțile interesate relevante să le ia în considerare când evaluează serviciile de cloud și colaborează cu furnizorii de servicii de cloud[4]. Deși, pentru majoritatea acestor puncte, amploarea obligațiilor impuse de RGPD este clară atât pentru operatori, cât și pentru persoanele împuternicite de operatori, potrivit AS DK, amploarea exactă a anumitor obligații în temeiul RGPD rămâne neclară[5].

   AS DK a pus următoarele întrebări:

4. Întrebarea 1.1: Luând în considerare articolul 5 alineatul (2) și articolul 24 alineatul (1) din RGPD, în cazul în care se recurge la o persoană împuternicită de operator care să efectueze prelucrarea în numele operatorului, pentru a documenta conformitatea, printre altele, cu articolul 28 alineatul (1) și articolul 28 alineatul (2) (inclusiv când se prezintă documentația la AS la inspecție):

   a. Operatorul trebuie să identifice toți subcontractanții persoanei împuternicite de operator, subcontractanții acestora etc. de-a lungul întregului lanț de prelucrare sau să identifice doar prima linie de subcontractanți angajați de persoana împuternicită de operator?

   b. În ce măsură și cât de detaliat trebuie să verifice și să documenteze operatorul:

      i. suficiența garanțiilor oferite de persoanele împuternicite de operator, subcontractanții lor etc.,
      ii. conținutul contractelor dintre persoana împuternicită inițială și persoanele împuternicite suplimentare pentru a verifica dacă aceleași obligații au fost impuse persoanelor împuternicite de operator suplimentare conform articolului 28 alineatul (4) din RGPD; și
      iii. dacă persoanele împuternicite de operator, subcontractanții lor etc. îndeplinesc cerințele operatorului prevăzute la articolul 28 alineatul (1)?

5. Întrebarea 1.2: În cazul transferurilor sau al transferurilor ulterioare de la o persoană împuternicită de operator (subcontractant) la altă persoană împuternicită de operator (subcontractant) în conformitate cu instrucțiunile operatorului: În ce măsură trebuie operatorul, ca parte a obligației care îi revine în temeiul articolului 28 alineatul (1) din RGPD, coroborat cu articolul 44 din RGPD, să evalueze și să fie în măsură să prezinte documente de la persoanele împuternicite de operator (subcontractanți) care să ateste că nivelul de protecție a datelor cu caracter personal nu este subminat de transferurile (ulterioare)?

[2] Raport privind acțiunea coordonată de asigurare a respectării legislației din 2022 – Utilizarea serviciilor bazate pe cloud de către sectorul public, 17 ianuarie 2023 (denumit în continuare „Raportul MIE privind serviciile de cloud").

[3] Cadrul coordonat de asigurare a respectării normelor a fost instituit de CEPD în octombrie 2020 în vederea raționalizării aplicării legislației și cooperării între autoritățile de supraveghere. Vezi documentul CEPD privind cadrul coordonat de punere în aplicare în temeiul Regulamentului 2016/679, adoptat la 20 octombrie 2020, versiunea 1.1.

[4] Raportul MIE privind serviciile de cloud, p. 10-20.

[5] Cerere, p. 1.

6. Întrebarea 1.3: Întinderea obligațiilor prevăzute la articolul 28 alineatul (1) și la articolul 28 alineatul (2) din RGPD coroborate cu articolul 5 alineatul (2) și cu articolul 24 din RGPD, astfel cum s-a răspuns la întrebarea 1.1 și la întrebarea 1.2, variază în funcție de riscul asociat activității de prelucrare? Dacă da, care este amploarea acestor obligații pentru activitățile de prelucrare cu risc scăzut și care este amploarea pentru activitățile de prelucrare cu risc mare?

7. Întrebarea nr. 2: Un contract sau alt act juridic în temeiul dreptului Uniunii sau al dreptului intern în temeiul articolului 28 alineatul (3) din RGPD trebuie să conțină excepția prevăzută la articolul 28 alineatul (3) litera (a), „*cu excepția cazului în care această obligație îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică*" (textual sau în termeni foarte similari) pentru a fi în conformitate cu RGPD?

8. Întrebarea 2a: dacă răspunsul la întrebarea 2 este negativ, în cazul în care un contract sau alt act juridic în temeiul dreptului Uniunii sau al dreptului intern care extinde excepția de la articolul 28 alineatul (3) litera (a) din RGPD pentru a acoperi și legislația țării terțe în general (de exemplu „cu excepția cazului în care această obligație îi revine în temeiul legii sau al unei ordonanțe obligatorii a unui organism guvernamental"), este acest lucru în sine o încălcare a articolului 28 alineatul (3) litera (a) din RGPD?

9. Întrebarea 2b: Dacă răspunsul la întrebarea 2a este negativ, o astfel de excepție extinsă ar trebui interpretată ca instrucțiune documentată a operatorului în sensul articolului 28 alineatul (3) litera (a) din RGPD?

1.2 Admisibilitatea cererii de emitere a unui aviz în temeiul articolului 64 alineatul (2) din RGPD

10. Articolul 64 alineatul (2) din RGPD prevede, în special, că orice autoritate de supraveghere, președintele Comitetului sau Comisia poate solicita ca orice chestiune de aplicare generală sau care produce efecte în mai mult de un stat membru să fie examinată de Comitet în vederea obținerii unui aviz.

11. Primele întrebări adresate de AS DK se referă la obligațiile de răspundere ale operatorilor în temeiul articolului 28 din RGPD (întrebările 1.1, 1.2 și 1.3), iar ultima întrebare se referă la conținutul specific al contractului sau al actului juridic al operatorului/persoanei împuternicite de operator în temeiul articolului 28 alineatul (3) litera (a) din RGPD (întrebarea 2).

12. Comitetul consideră că aceste întrebări sunt legate de interpretarea RGPD, în special în ceea ce privește relația dintre operatori și persoanele împuternicite de operator (subcontractanții) lor, precum și interpretarea articolului 5 alineatul (2), a articolului 24 și a articolului 28 din RGPD. Solicitarea este legată, pe de o parte, de obligațiile de răspundere ale operatorilor și de nivelul de documentare pe care autoritățile de supraveghere ar trebui să-l aștepte de la operatorii care recurg la persoane împuternicite de operator (subcontractanți) pentru a efectua activități de prelucrare în numele lor și, pe de altă parte, de conținutul contractelor sau actelor juridice între operatori și persoane împuternicite de operator. Prin urmare, această cerere privește o „*chestiune de aplicare generală*" în sensul articolului 64 alineatul (2) din RGPD.

13. În plus, Comitetul consideră că cererea AS DK este motivată conform articolului 10 alineatul (3) din Regulamentul de procedură al CEPD, întrucât AS DK a furnizat argumente în favoarea necesității unei interpretări coerente a întrebărilor abordate în cerere.

14. Conform articolului 64 alineatul (3) din RGPD, CEPD nu emite un aviz dacă a emis deja un aviz pe această temă[6]. CEPD nu a furnizat încă răspunsuri la întrebările care decurg din solicitarea AS DK. În plus, orientările disponibile ale CEPD, inclusiv, în special, Orientările nr. 7/2020 ale CEPD privind conceptele de operator și de persoană împuternicită de operator[7] (denumite în continuare „Orientările nr. 7/2020 ale CEPD"), oferă unele îndrumări cu privire la amploarea obligațiilor de asumare a răspunderii ale operatorului în temeiul articolului 28 din RGPD, dar orientările existente nu abordează pe deplin toate întrebările prezentate în cerere[8]. Mai precis, de exemplu, orientările disponibile cu privire la articolul 28 alineatul (3) litera (a) din RGPD nu abordează în mod specific întrebarea din cererea AS DK cu privire la nevoia de includere în contractele sau actele juridice dintre operatori și persoanele împuternicite de operatori a termenilor *„cu excepția cazului în care această obligație îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică"* ar trebui incluși în contractele sau actele juridice dintre operatori și persoanele împuternicite de operatori.

15. Din aceste motive, Comitetul consideră că cererea AS DK este admisibilă, iar întrebările care decurg din cererea AS DK trebuie analizate într-un aviz adoptat în conformitate cu articolul 64 alineatul (2) din RGPD.

2 CU PRIVIRE LA TEMEINICIA CERERIIERROR! BOOKMARK NOT DEFINED.

2.1 Cu privire la interpretarea articolului 28 alineatul (1), a articolului 28 alineatul (2) și a articolului 28 alineatul (4) din RGPD coroborate cu articolul 5 alineatul (2) și cu articolul 24 alineatul (1) (întrebările 1.1 și 1.3)

16. Această secțiune abordează întrebările 1.1 și 1.3 adresate Comitetului, astfel cum sunt reproduse în secțiunea „Admisibilitate" de mai sus.

17. Articolul 28 din RGPD stabilește relația dintre operator și persoana împuternicită de operator și impune obligații directe operatorilor și persoanelor împuternicite de operator. Ca observație preliminară, trebuie remarcat că RGPD definește „persoana împuternicită de operator" la articolul 4 alineatul (8) într-un mod general care include atât persoana împuternicită inițială angajată direct de operator, cât și persoana împuternicită de operator și așa mai departe de-a lungul lanțului de prelucrare.

18. CEPD subliniază că evaluarea rolului părților (și dacă acestea acționează ca operatori unici sau asociați sau ca persoane împuternicite de operatori) nu intră în obiectul cererii. CEPD reamintește că este, în primul rând, de competența părților să-și evalueze rolul real în funcție de elementele de fapt sau de circumstanțele cazului[9], fără a aduce atingere competenței AS de a verifica dacă evaluarea lor este adevărată.

[6] Articolul 64 alineatul (3) din RGPD și articolul 10 alineatul (4) din Regulamentul de procedură al CEPD.
[7] CEPD, Orientările nr. 7/2020 privind conceptele de operator de date și persoană împuternicită de operator în cadrul RGPD, 2.1, adoptate la 7 iulie 2021.
[8] Vezi în special Orientările CEPD nr. 7/2020, secțiunea 1.1 „Alegerea persoanei împuternicite de operator" la pagina 30, secțiunea 1.3.4 *„Persoana împuternicită de operator trebuie să respecte condițiile menționate la articolul 28 alineatele (2) și (4) pentru recrutarea altei persoane împuternicite de operator [articolul 28 alineatul (3) litera (d) din RGPD]"* la pagina 37, secțiunea 1.6 „Subcontractanți", la pagina 42.
[9] Orientările CEPD nr. 7/2020, punctul 12.

19. Având în vedere întrebările de mai sus, prezentul aviz se concentrează exclusiv asupra întinderii și amplorii obligațiilor operatorului prevăzute la articolul 28 alineatul (1) din RGPD, pentru a verifica dacă oferă „garanții suficiente", în conformitate cu articolul 28 alineatul (2), și a obligațiilor operatorului legate de responsabilitate, prevăzute la articolul 5 alineatul (2) și la articolul 24 alineatul (1) din RGPD[10].

20. În plus, Comitetul constată că întrebările de mai sus nu se referă la răspunderea operatorului față de persoanele vizate pentru activitățile de prelucrare efectuate în numele său, de exemplu în ceea ce privește dreptul persoanelor vizate la despăgubiri în temeiul articolului 82 din RGPD. Prin urmare, această secțiune se va concentra pe furnizarea de clarificări autorităților de supraveghere în ceea ce privește interpretarea articolului 28 alineatul (1) și a articolului 28 alineatul (2) din RGPD, combinate cu articolul 5 alineatul (2) și cu articolul 24 din RGPD, cu privire la anumite obligații care decurg din folosirea de persoane împuternicite de operator și de subcontractanți. Pentru a răspunde la aceste întrebări, Comitetul va efectua o analiză axată pe situațiile în care nu există niciun transfer de date cu caracter personal în afara SEE. În schimb, secțiunea de mai jos privind întrebarea 1.2 evaluează situațiile în care au loc transferuri de-a lungul lanțului de prelucrare.

2.1.1 Identificarea actorilor din lanțul de prelucrare

21. În ceea ce privește întrebarea dacă, în esență, operatorul trebuie să identifice toți subcontractanții persoanei împuternicite de operator, subcontractanții lor etc. de-a lungul lanțului de prelucrare sau trebuie să identifice doar prima linie de subcontractanți angajați de persoana împuternicită de operator, CEPD reamintește, în primul rând, că *„Deși lanțul [de prelucrare] poate fi destul de lung, operatorul își păstrează rolul central în determinarea scopului și mijloacelor de prelucrare"*[11].

22. CEPD interpretează termenii „identificare" și „informații privind identitatea" în scopul de a răspunde la întrebare ca referindu-se la numele, adresa, persoana de contact (nume, funcție, date de contact) a persoanei împuternicite de operator și la descrierea prelucrării (inclusiv delimitarea clară a responsabilităților în caz că sunt autorizați mai mulți subcontractanți)[12].

23. În ceea ce privește alegerea persoanelor împuternicite de operator, operatorii trebuie să fie într-o poziție care să le permită să determine în mod eficient scopurile și mijloacele prelucrării, conform articolului 4 alineatul (7) din RGPD. În acest sens, determinarea destinatarilor (inclusiv a persoanelor împuternicite de operator) este considerată un „mijloc esențial" al prelucrării, cu privire la care decide operatorul[13].

24. În acest scop, în ceea ce privește angajarea de **subcontractanți suplimentari** de către persoana împuternicită inițială, este necesară autorizarea scrisă prealabilă specifică sau generală a operatorului

[10] Această întrebare este distinctă și separată de alte obligații ale operatorului [sau ale persoanei împuternicite de operator (subcontractanților)] de a asigura conformitatea cu RGPD, de exemplu cu principiul legalității, cu articolul 32 sau cu obligațiile prevăzute la capitolul V din RGPD. Operatorul poate fi în continuare responsabil de prelucrarea în cadrul controlului său care nu este în conformitate cu aceste dispoziții din RGPD, chiar dacă și-a îndeplinit obligațiile de a verifica persoanele împuternicite de operator (subcontractanți) în conformitate cu articolul 28 alineatul (1) din RGPD, detaliate în prezentul aviz, iar prezentul aviz nu abordează responsabilitatea operatorului în ceea ce privește respectarea altor dispoziții din RGPD decât articolul 24 alineatul (1), articolul 28 alineatul (1) și articolul 28 alineatul (2) din RGPD.

[11] Orientările CEPD nr. 7/2020, punctul 152.

[12] Acest lucru reflectă informațiile necesare pentru identificarea persoanelor împuternicite de operatori din anexa IV la CCS privind operatorii/persoanele împuternicite de operatori ale Comisiei Europene (Decizia de punere în aplicare 2021/915 a Comisiei din 4 iunie 2021) și din anexa III la CCS privind transferurile internaționale ale Comisiei Europene (Decizia de punere în aplicare 2021/914 a Comisiei din 4 iunie 2021).

[13] Orientările CEPD nr. 7/2020, punctul 40.

în temeiul articolului 28 alineatul (2) din RGPD. Orientările CEPD nr. 7/2020 introduc obligații specifice prevăzute la articolul 28 alineatul (2) *„care se declanșează atunci când un subcontractant intenționează să angajeze un alt actor, adăugând astfel o altă verigă în lanț, prin atribuirea de activități care necesită prelucrarea datelor cu caracter personal."*[14]

25. În cazurile în care operatorul decide să accepte anumiți subcontractanți în momentul semnării contractului, trebuie inclusă în contract sau într-o anexă la acesta o listă a subcontractanților aprobați. Lista trebuie apoi actualizată, în conformitate cu autorizația generală sau specifică acordată de operator.[15]

26. În ceea ce privește angajarea subcontractanților, RGPD prevede posibilitatea unei autorizații generale sau specifice. **În cazul unei autorizații specifice**, operatorul trebuie să specifice în scris ce subcontractant este autorizat, pentru ce activitate de prelucrare specifică și pentru ce perioadă[16]. Dacă cererea de autorizare specifică a persoanei împuternicite de operator nu primește răspuns în termenul stabilit, aceasta trebuie considerată respinsă[17].

27. **În cazul unei autorizații generale**, persoana împuternicită de operator trebuie să dea operatorului posibilitatea să aprobe o listă a subcontractanților în momentul semnării autorizației generale, precum și posibilitatea de a se opune oricăror schimbări ulterioare ale subcontractanților, inclusiv într-un interval de timp suficient[18]. Comitetul reamintește că ar trebui să fie la latitudinea **persoanei împuternicite inițiale să furnizeze în mod proactiv anumite informații** operatorului, iar *„obligația persoanei împuternicite de operator de a-l informa pe acesta cu privire la orice schimbare a subcontractanților implică faptul că persoana împuternicită de operator indică sau semnalează **în mod activ** astfel de modificări pentru operator."*[19].

28. Asta înseamnă că informațiile referitoare la identificarea tuturor subcontractanților persoanei împuternicite de operator trebuie să fie ușor accesibile operatorului. Identificarea acestor actori este deosebit de relevantă pentru ca operatorul să poată avea control asupra activităților sale de prelucrare pentru care este responsabil și poate fi tras la răspundere în cazul unei încălcări a RGPD.

[14] Punctul 151 din Orientările CEPD nr. 7/2020 prevede: *„Activitățile de prelucrare a datelor sunt adesea efectuate de un număr mare de actori, iar lanțurile de subcontractare devin din ce în ce mai complexe. RGPD introduce obligații specifice care se declanșează atunci când un subcontractant intenționează să angajeze un alt actor, adăugând astfel o altă verigă în lanț, prin atribuirea de activități care necesită prelucrarea datelor cu caracter personal. Analiza dacă furnizorul de servicii acționează ca subcontractant trebuie efectuată în conformitate cu cele descrise anterior în legătură cu conceptul de persoană împuternicită de operator"*.

[15] Orientările CEPD nr. 7/2020, punctul 154.

[16] Orientările CEPD nr. 7/2020, punctele 153 și 155. În conformitate cu clauza 7.7, opțiunea 1, din CCS CE operator-persoana împuternicită de operator, lista subcontractanților autorizați în mod specific de operator trebuie să se regăsească în anexa IV, care trebuie ținută la zi.

[17] Orientările CEPD nr. 7/2020, punctul 155.

[18] Vezi și Orientările CEPD nr. 7/2020, punctul 156. *„Alternativ, operatorul poate acorda o autorizație generală pentru utilizarea subcontractanților (în contract, inclusiv o listă cu astfel de subcontractanți într-o anexă la acesta) (...)*". De asemenea, relevant în acest context este Avizul CEPD nr. 14/2019 privind proiectul de clauze contractuale standard înaintat de AS DK [articolul 28 alineatul (8) din RGPD]. Conform clauzei 7.7 opțiunea 2 din CCS-urile Comisiei Europene operator-persoana împuternicită de operator, persoana împuternicită de operator deține autorizația generală a operatorului pentru recrutarea de subcontractanți dintr-o listă convenită și informează în mod specific, în scris, operatorul cu privire la modificările preconizate ale listei respective prin adăugarea sau înlocuirea în prealabil a subcontractanților.

[19] Orientările CEPD nr. 7/2020, punctul 128 (subliniere adăugată). Vezi și nota de subsol 14.

29. Prin urmare, persoana împuternicită de operator trebuie să furnizeze toate informațiile privind modul în care va fi efectuată activitatea de prelucrare în numele operatorului, inclusiv informații despre subcontractantul utilizat[20] și o descriere a prelucrării care este încredințată subcontractantului[21].

30. Alte motive juridice justifică necesitatea ca operatorul să identifice toate persoanele împuternicite de operator și subcontractanții. Persoanele împuternicite de operator cărora le sunt divulgate sau transferate date sunt considerate „destinatari"[22].

- Pentru a respecta cerințele de transparență prevăzute la articolul 13 alineatul (1) litera (e) și la articolul 14 alineatul (1) litera (e) din RGPD, operatorii trebuie să informeze persoanele vizate cu privire la destinatarii sau categoriile de destinatari ai datelor, fiind cât mai specifici și concreți posibil[23]. Informațiile privind „categoriile de destinatari" trebuie, de asemenea, incluse în înregistrările de prelucrare [articolul 30 alineatul (1) litera (d)].

- Articolul 15 din RGPD prevede, printre altele, dreptul de acces la informații privind destinatarii sau categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal[24]. Curtea de Justiție a clarificat că această dispoziție implică obligația operatorului de a furniza persoanei vizate identitatea reală a destinatarilor[25]. În afara tipului de cazuri, în care operatorul poate indica persoanei vizate numai

[20] Orientările CEPD nr. 7/2020, punctul 143.

[21] Vezi, de exemplu, anexa IV la CCS CE operator -persoană împuternicită de operator și anexa II la CCS CE pentru transferuri internaționale.

[22] Articolul 4 alineatul (9) din RGPD; Orientările GL29 privind transparența în temeiul Regulamentului 2016/679, adoptate la 29 noiembrie 2017, astfel cum au fost revizuite și adoptate ultima dată la 11 aprilie 2018, WP260 rev.01, aprobate de CEPD (denumite în continuare „Orientările GL29 privind transparența"), p. 37.

[23] Orientările GL29 privind transparența, p. 37 („*În conformitate cu principiul echității, operatorii trebuie să furnizeze informații cu privire la destinatari, care sunt cele mai semnificative pentru persoanele vizate. În practică, aceștia vor fi numiți, în general, destinatari, astfel încât persoanele vizate să știe exact cine deține datele lor cu caracter personal. Dacă operatorii aleg să prezinte categoriile de destinatari, informațiile trebuie să fie cât mai precise, indicând tipul de destinatari (și anume, prin trimitere la activitățile pe care le desfășoară aceștia), industria, sectorul și subsectorul, precum și localizarea destinatarilor.*"); Orientările CEPD nr. 1/2022 privind drepturile persoanelor vizate - Dreptul de acces, versiunea 2.1, adoptate la 28 martie 2023, [denumite în continuare „Orientările CEPD nr. 1/2022 (dreptul de acces)"], punctul 117 („*deja în temeiul articolelor 13 și 14 din RGPD, informațiile privind destinatarii sau categoriile de destinatari ar trebui să fie cât mai concrete posibil, cu respectarea principiilor transparenței și corectitudinii*"); vezi CJUE, hotărârea din 12 ianuarie 2023, *RW/Österreichische Post AG*, C-154/21, punctul 25; Avizul AG privind CJUE C-154/21, punctul 36 („*Articolele 13 și 14 din RGPD [...] care stabilesc o obligație în sarcina operatorului de a furniza persoanei vizate informațiile referitoare la categoriile de destinatari sau la destinatarii concreți ai datelor cu caracter personal care o privesc atunci când acestea sunt sau nu sunt colectate de la persoana vizată*").

[24] Articolul 5 alineatul (1) litera (c) din RGPD. Orientările CEPD nr. 1/2022 (dreptul de acces), punctele 116-117.

[25] Hotărârea CJUE din 12 ianuarie 2023, *RW/Österreichische Post AG*,C-154/21, punctul 51: „*Articolul 15 alineatul (1) litera (c) din RGPD trebuie interpretat în sensul că dreptul de acces al persoanei vizate la datele cu caracter personal care o privesc, prevăzut de această dispoziție, implică, atunci când aceste date le-au fost sau urmează să le fie divulgate unor destinatari, obligația operatorului de a-i furniza acestei persoane identitatea însăși a acestor destinatari, cu excepția cazului în care este imposibil să se identifice acești destinatari sau a cazului în care operatorul menționat demonstrează că cererile de acces ale persoanei vizate sunt în mod vădit nefondate sau excesive, în sensul articolului 12 alineatul (5) din RGPD, cazuri în care acesta îi poate indica acestei persoane numai categoriile de destinatari în cauză*".
Curtea a recunoscut că persoana vizată poate, de asemenea, „*alege să se limiteze la a solicita informații privind categoriile de destinatari*". Hotărârea CJUE din 12 ianuarie 2023, *RW/Österreichische Post AG*, C-154/21, punctul 43.
Orientările CEPD nr. 1/2022 (dreptul de acces), punctul 117.

categoriile de destinatari, în principiu ar trebui să fie întotdeauna posibil ca operatorul să extragă numele destinatarilor și să furnizeze informațiile necesare persoanelor vizate fără întârzieri nejustificate.

- Articolul 19 din RGPD prevede că operatorul comunică fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal orice rectificare sau ștergere a datelor cu caracter personal sau restricționare a prelucrării, cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate. CJUE a clarificat că articolul 19 a doua teză conferă în mod expres persoanei vizate dreptul de a fi informată cu privire la destinatarii specifici[26].

31. Deși nu este explicit în aceste dispoziții, Comitetul consideră că, în sensul articolului 28 alineatul (1) și al articolului 28 alineatul (2) din RGPD, operatorii trebuie să aibă acces imediat, oricând, la informațiile privind identitatea tuturor persoanelor împuternicite de operatori, a subcontractanților etc.[27], ca să-și poată îndeplini cel mai bine obligațiile care le revin în temeiul dispozițiilor menționate mai sus. Această disponibilitate este, de asemenea, necesară pentru ca operatorii să poată colecta și evalua toate informațiile necesare pentru a îndeplini cerințele prevăzute de RGPD, inclusiv pentru a putea răspunde fără întârzieri nejustificate la cererile de acces în temeiul articolului 15 din RGPD și pentru a reacționa rapid la încălcările securității datelor care au loc de-a lungul lanțului de prelucrare. Acest lucru s-ar aplica indiferent de riscul asociat activității de prelucrare.

32. În acest scop, persoana împuternicită de operator trebuie să furnizeze în mod proactiv[28] operatorului toate informațiile privind identitatea tuturor persoanelor împuternicite de operator, a subcontractanților etc. care efectuează prelucrarea în numele operatorului și trebuie să actualizeze în permanență aceste informații cu privire la toți subcontractanții implicați. Operatorul și persoana împuternicită de operator pot include în contract detalii suplimentare cu privire la modul și formatul în care persoana împuternicită de operator trebuie să furnizeze aceste informații, deoarece operatorul poate dori să solicite un format specific, astfel încât operatorului să-i fie mai ușor să le recupereze și să le organizeze.

2.1.2 Verificarea și documentarea de către operator a suficienței garanțiilor oferite de toate persoanele împuternicite de operator din lanțul de prelucrare

33. Întrebările 1.1.b.i, 1.1.b.iii și 1.3 urmăresc să ofere clarificări cu privire la măsura și nivelul de detaliu în care operatorul trebuie să verifice și să documenteze caracterul suficient al garanțiilor oferite de toate persoanele împuternicite de operatori din lanțul de prelucrare și în ce măsură obligațiile prevăzute la articolul 28 alineatul (1) și la articolul 28 alineatul (2) din RGPD coroborate cu articolul 5 alineatul (2) și cu articolul 24 din RGPD variază în funcție de riscul asociat activității de prelucrare. În ceea ce privește aceste întrebări, Comitetul subliniază următoarele elemente.

34. Articolul 5 alineatul (2) din RGPD consacră principiul responsabilității, făcând operatorul responsabil de respectarea principiilor de protecție a datelor prevăzute la articolul 5 alineatul (1) din RGPD și de

[26] Hotărârea CJUE din 12 ianuarie 2023, *RW/ Österreichische Post AG*,C-154/21, punctul 41.

[27] Aceste informații sunt necesare pentru ca operatorul să-și poată îndeplini obligațiile și în cazul în care lanțul de subcontractare este întrerupt deoarece o persoană împuternicită de operator (subcontractant) este inaccesibilă, nedorită sau insolvabilă și trebuie contactată altă persoană împuternicită de operator (subcontractant).

[28] Pentru a respecta articolul 28 alineatul (2) din RGPD, pentru a permite operatorului să decidă cu privire la adăugarea de subcontractanți, precum și să respecte articolul 28 alineatul (1) din RGPD, pentru a permite operatorului să verifice dacă persoanele împuternicite de operator (subcontractanții) prezintă garanții suficiente pentru a pune în aplicare măsurile tehnice și organizatorice.

capacitatea de a demonstra această respectare. Articolul 5 alineatul (2) din RGPD se aplică tuturor principiilor generale enumerate la articolul 5 alineatul (1) din RGPD.

35. Articolul 24 alineatul (1) din RGPD include obligația operatorului de a demonstra că prelucrarea este efectuată în conformitate cu RGPD, dar dezvoltă în continuare una dintre atribuțiile la care se aplică principiul responsabilității: punerea în aplicare de „măsuri tehnice și organizatorice adecvate "[29]. Articolul 24 alineatul (1) din RGPD se referă la noțiunea de „risc"[30] ca fiind relevantă pentru aplicarea sa, ca unul dintre criteriile pe care operatorul trebuie să le ia în considerare în evaluarea caracterului adecvat al acestor măsuri[31]. Articolul 24 alineatul (1) din RGPD adaugă, de asemenea, că aceste măsuri trebuie revizuite și actualizate, dacă este necesar.

36. După cum a afirmat CJUE, *„Articolul 5 alineatul (2) și articolul 24 din RGPD impun operatorilor de date cu caracter personal obligații generale de responsabilitate și de conformitate. În special, aceste dispoziții impun operatorilor să adopte măsurile adecvate pentru a preveni eventualele încălcări ale normelor prevăzute de RGPD pentru a asigura dreptul la protecția datelor"[32].*

37. Principiul responsabilității se adresează operatorului, inclusiv când operatorul a încredințat operatorilor sau subcontractanților prelucrarea datelor cu caracter personal în numele său.

38. În conformitate cu articolul 28 alineatul (1) din RGPD, când angajează o persoană împuternicită de operator pentru a efectua prelucrarea datelor cu caracter personal în numele său, operatorul trebuie să utilizeze numai o persoană împuternicită de operator care poate oferi *„garanții suficiente pentru*

---

[29] Hotărârea din 25 ianuarie 2024, *BL/MediaMarktSaturn Hagen-Iserlohn GmbH*, C-687/21, ECLI:EU:C:2024:72, punctul 36: *„Articolul 24 din RGPD prevede o obligație generală ce revine operatorului de date cu caracter personal de a pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și pentru a putea demonstra că prelucrarea se efectuează în conformitate cu acest regulament*".

[30] Considerentul 75 din RGPD enumeră câteva exemple de riscuri: *„prelucrarea poate conduce la discriminare, furt sau fraudă a identității, pierdere financiară, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional, inversarea neautorizată a pseudonimizării sau la orice alt dezavantaj semnificativ de natură economică sau socială"*; Considerentul 76 precizează: *Probabilitatea de a se materializa și gravitatea riscului pentru drepturile și libertățile persoanei vizate ar trebui să fie determinate în funcție de natura, domeniul de aplicare, contextul și scopurile prelucrării datelor cu caracter personal*. *Riscul ar trebui apreciat pe baza unei evaluări obiective prin care se stabilește dacă operațiunile de prelucrare a datelor prezintă un risc sau un risc ridicat.*" După cum a rezumat CJUE, *„potrivit considerentului 76 al acestui regulament, probabilitatea și gravitatea riscului depind de particularitățile tratamentului în cauză, iar acest risc ar trebui apreciat pe baza unei evaluări obiective.*" (CJUE, hotărârea din 14 decembrie 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, par. 36).

[31] După cum a afirmat CJUE, *„articolul 24 alineatul (1) enumeră o serie de criterii care trebuie luate în considerare la evaluarea caracterului adecvat al unor astfel de măsuri, și anume natura, domeniul de aplicare, contextul și scopul prelucrării, precum și riscurile de probabilitate și gravitate diferite pentru drepturile și libertățile persoanelor fizice*", Hotărârea din 14 decembrie 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, punctul 25. În aceeași hotărâre, CJUE a precizat că *„Caracterul adecvat al unor asemenea măsuri trebuie evaluat în mod concret, examinând dacă aceste măsuri au fost implementate de acest operator ținând seama de diferitele criterii prevăzute (...) și de nevoile de protecție a datelor inerente în mod specific prelucrării în cauză, precum și riscurilor pe care le presupune aceasta din urmă*", punctul 30; amintit și în hotărârea din 25 ianuarie 2024, *BL/MediaMarktSaturn Hagen-Iserlohn GmbH*, C-687/21, ECLI:EU:C:2024:72, punctul 38: *„Astfel, din modul de redactare a articolelor 24 și 32 din RGPD reiese că caracterul adecvat al măsurilor implementate de operator trebuie evaluat în mod concret, ținând seama de diferitele criterii prevăzute la aceste articolele și de nevoile de protecție a datelor inerente în mod specific prelucrării în cauză, precum și riscurile pe care le presupune aceasta din urmă, cu atât mai mult cu cât operatorul menționat trebuie să fie în măsură să demonstreze conformitatea cu acest regulament a măsurilor respective, posibilitate de care ar fi privat dacă s-ar admite o prezumție irefragabilă*". Trebuie remarcat că analiza CJUE se referă și la articolul 32 din RGPD.

[32] Hotărârea din 27 octombrie 2022, *Proximus NV/Gegevensbeschermingsautoriteit*, C-129/21, ECLI:EU:C:2022:833, punctul 81. Vezi și Orientările CEPD 07/2020, punctul 9.

punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte cerințele" din RGPD „*și să asigure protecția drepturilor persoanei vizate*"[33]. După cum se indică în Orientările CEPD nr. 7/2020, principiul responsabilității este reflectat și în articolul 28 din RGPD[34].

39. În acest sens, CEPD subliniază că, în scopul evaluării conformității cu articolul 24 alineatul (1) și cu articolul 28 alineatul (1) din RGPD, autoritățile de supraveghere ar trebui să considere că **recrutarea persoanelor împuternicite de operator nu trebuie să reducă nivelul de protecție a drepturilor persoanelor vizate** în comparație cu o situație în care prelucrarea este efectuată direct de operator. Aceasta se referă la angajarea persoanei împuternicite inițiale, dar și la angajarea de persoane împuternicite suplimentare de-a lungul lanțului de prelucrare, de exemplu subcontractanți și sub-subcontractanți. Articolul 24 alineatul (1) și articolul 28 alineatul (1) din RGPD trebuie interpretate în sensul că impun operatorului să se asigure că lanțul de prelucrare este format numai din persoane împuternicite de operator, subcontractanți, sub-subcontractanți (etc.) care oferă „garanții suficiente pentru a pune în aplicare măsuri tehnice și organizatorice adecvate". În plus, operatorul trebuie să poată dovedi că a luat în considerare cu seriozitate toate elementele prevăzute în RGPD[35]. Aceste considerente sunt adevărate chiar dacă lanțul de prelucrare poate fi lung și complex, având persoane împuternicite de operator, subcontractanți etc. diferite, care sunt implicate în diferite etape ale activităților de prelucrare. Operatorul trebuie să exercite diligența necesară în selectarea și supravegherea persoanelor împuternicite de operator.

40. În ceea ce privește alegerea **persoanei împuternicite inițiale**, operatorul ar trebui să verifice dacă garanțiile furnizate sunt suficiente de la caz la caz, ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile pentru drepturile și libertățile persoanelor fizice, pe baza tipului de prelucrare încredințată persoanei împuternicite de operator[36]. În conformitate cu articolul 28 alineatul (5) din RGPD, aderarea unei persoane împuternicite de operator la un cod de conduită aprobat în temeiul articolului 40 din RGPD sau la un mecanism de certificare aprobat în temeiul articolului 42 din RGPD poate fi utilizată ca element prin care să se demonstreze existența unor garanții suficiente.

41. După cum a menționat anterior CEPD, operatorul ar trebui să ia în considerare mai multe elemente când verifică garanțiile oferite de persoana împuternicită de operator[37], iar un schimb de documente relevante va fi adesea necesar[38]. În orice caz, „[*g*]*aranțiile „oferite" de persoana împuternicită de operator sunt cele pe care persoana împuternicită de operator este în măsură să le demonstreze spre satisfacția operatorului, întrucât acestea sunt singurele care pot fi luate în considerare efectiv de către operator atunci când evaluează respectarea obligațiilor sale*"[39]. Nici articolul 28 alineatul (1) din RGPD în sine, nici documentele anterioare ale CEPD nu furnizează lista exhaustivă a documentelor sau a acțiunilor pe care persoana împuternicită de operator ar trebui să le prezinte sau să le demonstreze

[33] Orientările CEPD nr. 7/2020, punctul 94.
[34] Orientările CEPD nr. 7/2020, punctul 8.
[35] Orientările CEPD nr. 7/2020, punctul 94.
[36] Orientările CEPD nr. 7/2020, punctul 96.
[37] Orientările CEPD nr. 7/2020, punctele 97-98 (referitoare la cunoștințele de specialitate, fiabilitatea și resursele persoanei împuternicite de operator, precum și la reputația persoanei împuternicite de operator pe piață și la aderarea la un cod de conduită sau la un mecanism de certificare aprobat).
[38] Orientările CEPD nr. 7/2020, punctul 95 (unde se menționează, de exemplu, politica de confidențialitate, condițiile de utilizare, evidența activităților de prelucrare, politica de gestionare a evidențelor, politica de securitate a informațiilor, rapoartele auditurilor externe privind protecția datelor, certificările internaționale recunoscute, de exemplu seria ISO 27000).
[39] Orientările CEPD nr. 7/2020, punctul 95.

întrucât acest lucru depinde în mare măsură de circumstanțele specifice ale prelucrării[40]. De exemplu, operatorul poate alege să întocmească un chestionar ca mijloc de colectare a informațiilor de la persoana împuternicită de operator pentru a verifica garanțiile relevante, să solicite documentația relevantă, să se bazeze pe informații disponibile public și/sau pe certificări sau rapoarte de audit de la terți de încredere și/sau să efectueze audituri la fața locului.

42. CEPD a precizat deja că obligația de a utiliza numai persoane împuternicite de operator care „oferă garanții suficiente", prevăzută la articolul 28 alineatul (1) din RGPD, este o obligație continuă și că operatorul trebuie să verifice, la intervale adecvate, garanțiile persoanei împuternicite de operator[41].

43. Având în vedere întrebarea 1.3 ridicată de AS DK în cererea sa privind riscul asociat prelucrării, CEPD subliniază că noțiunea de risc joacă un rol important într-o serie de dispoziții ale RGPD, în special cele referitoare la capitolul IV din RGPD[42].

44. Este important de subliniat că trimiterea la „risc" de la articolul 24 alineatul (1) și de la considerentul 74 din RGPD nu trebuie interpretată în sensul că operatorul poate neglija sau se poate abate de la obligațiile care îi revin în temeiul RGPD pe baza simplei sale aprecieri a nivelului „scăzut" de risc pentru drepturile și libertățile persoanelor vizate. Obligația de a pune în aplicare „măsuri tehnice și organizatorice adecvate" pentru a asigura conformitatea cu RGPD în conformitate cu articolul 24 alineatul (1) din RGPD se aplică întotdeauna, dar măsurile care sunt necesare pentru a obține acest rezultat pot varia în funcție de risc[43].

45. Deși nu face trimiteri specifice la „risc", articolul 28 alineatul (1) din RGPD implică necesitatea de a lua în considerare nivelul riscului pentru drepturile și libertățile persoanelor vizate. Cerința prevăzută la articolul 28 alineatul (1) de a utiliza numai operatori care oferă „garanții suficiente" pentru a pune în aplicare „măsuri tehnice și organizatorice adecvate" trebuie interpretată ca implicând necesitatea de a lua în considerare furnizarea de către operatori a unor garanții suficiente pentru a pune în aplicare astfel de măsuri în lumina riscurilor prelucrării, deoarece, de exemplu, nivelul măsurilor de securitate care trebuie puse în aplicare depinde și de riscuri.

46. Riscul asociat activității de prelucrare joacă un rol important în determinarea caracterului adecvat al măsurilor tehnice și organizatorice, împreună cu celelalte criterii menționate la articolul 24 alineatul (1) din RGPD**[44]**. În funcție de nivelul de risc asociat activității de prelucrare (de exemplu, dacă se prelucrează categorii speciale de date cu caracter personal), operatorul poate defini măsuri tehnice și organizatorice mai stricte sau mai extinse. Prin urmare, orice persoană împuternicită de operator ar

[40] Orientările CEPD nr. 7/2020, punctul 96 („*Evaluarea de către operator a măsurii în care garanțiile sunt suficiente este o formă de evaluare a riscurilor, care va depinde în mare măsură de tipul de prelucrare atribuită persoanei împuternicite de operator și trebuie efectuată în fiecare caz individual, ținând seama de natura, domeniul de aplicare, contextul și de scopurile prelucrării, precum și de riscurile la adresa drepturilor și libertăților persoanelor fizice*. *În consecință, CEPD nu poate furniza o listă exhaustivă a documentelor sau a acțiunilor pe care persoana împuternicită de operator trebuie să le prezinte sau să le demonstreze în orice scenariu dat, deoarece acest fapt depinde în mare măsură de circumstanțele specifice ale prelucrării*").

[41] Orientările CEPD nr. 7/2020, punctul 99: „*inclusiv prin audituri și inspecții, după caz*".

[42] Termenul „risc" este menționat la articolele 24, 25, 27, 30, 32, 33, 34, 35, 36 și 39 din RGPD.

[43] CJUE, Hotărârea din 14 decembrie 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, punctul 35: „*considerentul 74 din RGPD subliniază că este important ca operatorul să fie obligat să pună în aplicare măsuri adecvate și eficace și să fie în măsură să demonstreze conformitatea activităților de prelucrare cu acest regulament, inclusiv eficacitatea măsurilor, care ar trebui să țină seama de criteriile referitoare la caracteristicile prelucrării în cauză și la riscul prezentat de aceasta, prevăzute la articolele 24 și 32*".

[44] Articolul 24 alineatul (1) se referă la „*natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice*".

trebui să ofere garanții suficiente pentru a pune în aplicare în mod eficace măsurile „adecvate” definite de operator.

47. Comitetul consideră că ***obligația*** **operatorului de a verifica dacă persoanele împuternicite de operator sau subcontractanții prezintă garanții suficiente pentru punerea în aplicare a măsurilor stabilite de operator ar trebui să se aplice indiferent de riscul pentru drepturile și libertățile persoanelor vizate.**

48. ***Amploarea*** **acestei verificări va varia însă în practică în funcție de natura acestor măsuri organizatorice și tehnice stabilite de operator pe baza, printre alte criterii, a riscului asociat prelucrării.** De exemplu, dacă activitățile de prelucrare prezintă un risc mai mic pentru drepturile și libertățile persoanelor vizate, „măsurile adecvate” corespunzătoare vor fi mai puțin stricte. Prin urmare, amploarea verificării operatorului poate fi mai puțin extinsă în practică. În schimb, în caz de riscuri mai mari care decurg din prelucrarea respectivă, nivelul de verificare al operatorului poate fi mai important în ceea ce privește verificarea garanțiilor suficiente prezentate de întregul lanț de prelucrare, având în vedere că „măsurile adecvate” care trebuie puse în aplicare sunt mai extinse și mai solide pentru a aborda riscurile pentru persoanele vizate.

49. În acest sens, în funcție de nivelul riscului asociat activității de prelucrare, operatorul poate mări nivelul de verificare verificând el însuși contractele de subcontractare a serviciilor de prelucrare a datelor și/sau poate impune, de asemenea, persoanei împuternicite inițiale o verificare și o documentație extinsă.

50. Conform principiului responsabilității, orice măsură care este considerată necesară pentru a respecta RGPD, inclusiv pe baza riscului pe care îl presupune prelucrarea, trebuie documentată în mod corespunzător de operator[45]. Această obligație este facilitată, pe de o parte, de **obligațiile de asistență și de audit** impuse persoanelor împuternicite de operatori și, pe de altă parte, de **informațiile furnizate operatorului de persoana împuternicită inițială** înainte de angajarea altor persoane împuternicite de operator.

51. În primul rând, Comitetul constată că persoanele împuternicite de operator au obligația de a asista operatorul în respectarea anumitor cerințe ale RGPD [în temeiul articolului 28 alineatul (3) literele (e) și (f)][46]. Mai general, persoana împuternicită de operator are obligația de a pune la dispoziția operatorului toate informațiile necesare pentru a demonstra conformitatea cu articolul 28 [articolul 28 alineatul (3) litera (h)][47]. Operatorul trebuie să fie pe deplin informat cu privire la detaliile prelucrării care sunt relevante pentru a demonstra conformitatea cu obligațiile prevăzute la articolul 28 din RGPD,

[45] În ceea ce privește sarcina probei atribuită operatorului, vezi CJUE, hotărârea din 14 decembrie 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, punctul 52 : „*Reiese fără ambiguitate din modul de redactare a articolului 5 alineatul (2), a articolului 24 alineatul (1) și a articolului 32 alineatul (1) din RGPD că sarcina de a dovedi că datele cu caracter personal sunt prelucrate într-un mod care asigură securitatea adecvată a acestora din urmă, în sensul articolului 5 alineatul (1) litera (f) și al articolului 32 din acest regulament, revine operatorului în cauză”*; vezi și Hotărârea CJUE din 25 ianuarie 2024, BL/MediaMarktSaturn Hagen-Iserlohn GmbH, C-687/21, ECLI:EU:C:2024:72, punctul 42 „*În această privință, trebuie să se sublinieze că din coroborarea articolelor 5, 24 și 32 din RGPD, interpretate în lumina considerentului (74) al acestuia, rezultă că, în cadrul unei acțiuni în despăgubire întemeiate pe articolul 82 din acest regulament, sarcina de a dovedi că datele cu caracter personal sunt prelucrate într-un mod care asigură securitatea adecvată a acestora din urmă, în sensul articolului 5 alineatul (1) litera (f) și al articolului 32 din regulamentul menționat, revine operatorului în cauză. O asemenea repartizare a sarcinii probei este de natură nu numai să încurajeze operatorii acestor date să adopte măsurile de securitate impuse de RGPD, ci și să asigure efectul util al dreptului la despăgubiri prevăzut la articolul 82 din acest regulament și să respecte intențiile legiuitorului Uniunii menționate în considerentul (11) al acestuia.*”

[46] Vezi Orientările CEPD nr. 7/2020, punctele 130-138.

[47] Vezi Orientările CEPD nr. 7/2020, punctele 143-145.

iar persoana împuternicită de operator trebuie să furnizeze toate informațiile privind modul în care activitatea de prelucrare este efectuată în numele operatorului[48]. Contractul trebuie să precizeze cât de des și cum ar trebui să aibă loc acest flux de informații[49].

52. Prin urmare, operatorul se poate baza pe informațiile furnizate de persoana împuternicită de operator, conform articolului 28 alineatul (3) litera (h) din RGPD, pentru a-și îndeplini obligația de documentare a măsurilor adoptate, cu condiția ca informațiile prezentate de persoana împuternicită de către operator să demonstreze efectiv conformitatea. Având în vedere că persoana împuternicită de operator este bine plasată pentru a cunoaște detaliile prelucrării pe care o efectuează și ale prelucrării efectuate de subcontractanți, aceasta trebuie să pună în mod proactiv la dispoziția operatorului toate informațiile relevante[50].

53. Cele de mai sus se aplică și subcontractanților. Într-adevăr, persoanele împuternicite de operator sunt obligate să transmită obligațiile de asistență de-a lungul lanțului de prelucrare [articolul 28 alineatul (4) din RGPD].

54. În al doilea rând, **recrutarea de subcontractanți,** după cum s-a amintit mai sus, este posibilă numai cu autorizarea scrisă prealabilă a operatorului, care poate fi specifică sau generală. Dacă operatorul alege să acorde autorizația sa generală, aceasta „*trebuie completată cu criterii care să orienteze alegerea persoanei împuternicite de operator (de exemplu, garanții în ceea ce privește măsurile tehnice și organizatorice, cunoștințele de specialitate, fiabilitatea și resursele)*”[51].

55. După cum explică CEPD, „*pentru a desfășura evaluarea și pentru a lua decizia dacă să autorizeze subcontractarea, operatorului de date va trebui să primească o listă a subcontractanților preconizați (care include în cazul fiecăruia: sediile acestora, ce acțiuni vor întreprinde și dovada garanțiilor care au fost puse în aplicare) de la persoana împuternicită de operator*”[52]. Aceste informații sunt necesare pentru ca operatorul să poată respecta principiul responsabilității prevăzut la articolul 5 alineatul (2) și articolul 24 și dispozițiile de la articolul 28 alineatul (1), de la articolul 32 și de la capitolul V din RGPD[53]. În ceea ce privește transferurile de date cu caracter personal în afara SEE, Comitetul face trimitere la răspunsul furnizat mai jos la întrebarea 1.2 adresată de AS DK.

56. După cum a reamintit CEPD, persoana împuternicită inițială trebuie să se asigure că propune subcontractanți care oferă garanții suficiente[54]. Necesitatea ca persoana împuternicită inițială de operator să furnizeze informațiile de mai sus arată că **persoana împuternicită de operator are un rol de jucat în alegerea subcontractanților și în verificarea garanțiilor pe care le oferă și trebuie să furnizeze operatorului informații suficiente**. Acest lucru concordă și cu faptul că, indiferent de

[48] Orientările CEPD nr. 7/2020, punctul 143.
[49] Orientările CEPD nr. 7/2020, punctul 143.
[50] Orientările CEPD nr. 7/2020, punctul 143, cu trimitere la articolul 28 alineatul (3) litera (h): „*De exemplu părțile relevante din evidențele activităților de prelucrare ale persoanei împuternicite de operator pot fi puse la dispoziția operatorului. Persoana împuternicită de operator trebuie să furnizeze toate informațiile cu privire la modul în care se va desfășura activitatea de prelucrare în numele operatorului. Aceste informații trebuie să includă informații privind funcționarea sistemelor utilizate, măsuri de securitate, modul în care sunt îndeplinite cerințele privind păstrarea datelor, localizarea datelor, transferurile de date, persoanele care au acces la date și care sunt destinatarii datelor, subcontractanții utilizați etc*.” Posibilitatea operatorului de a efectua un audit este, de asemenea, specificată la punctul 144: „*Scopul unui astfel de audit este să asigure că operatorul deține toate informațiile privind activitatea de prelucrare efectuată în numele său și garanțiile furnizate de persoana împuternicită de operator*.”
[51] Orientările CEPD nr. 7/2020, punctul 156.
[52] Orientările CEPD nr. 7/2020, punctul 152.
[53] Orientările CEPD nr. 7/2020, nota de subsol 69.
[54] Orientările CEPD nr. 7/2020, punctul 159.

criteriile sugerate de operator pentru a alege furnizorii, persoana împuternicită de operator rămâne pe deplin răspunzătoare față de operator în ceea ce privește îndeplinirea obligațiilor subcontractanților [articolul 28 alineatul (4) din RGPD].

57. În această privință, chiar dacă, în conformitate cu articolul 28 alineatul (4) din RGPD, este responsabilitatea directă a persoanei împuternicite de operator care angajează o persoană împuternicită de operator să se asigure că aceleași obligații în materie de protecție a datelor prevăzute în contractul inițial dintre operator și persoana împuternicită de operator sunt impuse acestei alte persoane împuternicite de operator, acest lucru nu înlătură responsabilitatea operatorului de a asigura conformitatea cu cerințele articolului 28 alineatul (1) și ale articolului 24 alineatul (1) din RGPD și de a fi în măsură să demonstreze această conformitate.

58. **Operatorului îi revine decizia finală cu privire la angajarea sau nu a unei anumite persoane împuternicite de operator sau a unui sub(sub)contractant și responsabilitatea corespunzătoare, inclusiv în ceea ce privește verificarea suficienței garanțiilor oferite de persoana împuternicită de operator sau de subcontractant.** După cum s-a reamintit deja, în cazul unei autorizații generice sau specifice, este întotdeauna la latitudinea operatorului să decidă dacă aprobă angajarea acestui subcontractant sau dacă se opune.

59. Atunci când evaluează conformitatea cu articolul 24 alineatul (1) și cu articolul 28 alineatul (1) din RGPD, autoritățile de supraveghere trebuie să evalueze dacă operatorul este în măsură să demonstreze că verificarea caracterului suficient al garanțiilor furnizate de subcontractanții săi a avut loc în mod satisfăcător pentru operator. Acest lucru înseamnă că operatorul poate alege să se bazeze pe informațiile primite de la persoana împuternicită de operator și, dacă este nevoie, să le dezvolte. De exemplu, în cazul în care informațiile primite de operator par incomplete, inexacte sau ridică semne de întrebare sau, după caz, în funcție de circumstanțele cazului, inclusiv de riscul asociat prelucrării, operatorul trebuie să solicite informații suplimentare și/sau să verifice informațiile și să le completeze/să le corecteze, dacă este nevoie.

60. Mai precis, pentru prelucrarea care prezintă un risc mare pentru drepturile și libertățile persoanelor vizate, operatorul trebui să-și sporească nivelul de verificare a informațiilor furnizate cu privire la garanțiile prezentate de diferitele persoane împuternicite de operatori din lanțul de prelucrare.

2.1.3 Verificarea contractului dintre persoana împuternicită inițială și persoanele împuternicite suplimentareError! Bookmark not defined.

61. AS DK întreabă, în esență, dacă și în ce măsură operatorul are obligația să verifice și să documenteze dacă contractele de subcontractare impun aceleași obligații persoanelor împuternicite suplimentare.

62. Articolul 28 alineatul (4)[55] impune o obligație directă în acest sens persoanelor împuternicite de operatori. În plus, articolul 28 alineatul (3) litera (d) impune operatorului și persoanei împuternicite de operator să „prevadă” obligația persoanei împuternicite de operator de a respecta condițiile menționate la articolul 28 alineatul (4) în contractul lor, făcând astfel din această cerință o obligație contractuală impusă persoanei împuternicite de operator. Cu alte cuvinte, **persoana împuternicită**

[55] Articolul 28 alineatul (4) din RGPD: *„În cazul în care o persoană împuternicită de un operator recrutează o altă persoană împuternicită pentru efectuarea de activități de prelucrare specifice în numele operatorului, aceleași obligații privind protecția datelor prevăzute în contractul sau în alt act juridic încheiat între operator și persoana împuternicită de operator, astfel cum se prevede la alineatul (3), revin celei de a doua persoane împuternicite, prin intermediul unui contract sau al unui alt act juridic, în temeiul dreptului Uniunii sau al dreptului intern, în special furnizarea de garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să îndeplinească cerințele prezentului regulament.”*

inițială este obligată, din punct de vedere juridic și contractual, să transfere aceleași obligații în materie de protecție a datelor în contractele de subcontractare pe care le încheie cu operatori suplimentari.

63. În mod similar, persoanelor împuternicite de operator suplimentare li se va solicita prin contract (de către persoana împuternicită inițială) să impună aceleași obligații de protecție a datelor asupra propriilor persoane împuternicite de operator și așa mai departe de-a lungul lanțului de prelucrare[56]. Nu este obligatoriu ca textul contractului de subcontractare a serviciilor de prelucrare a datelor să fie identic cu cel al contractului de prelucrare a datelor încheiat cu persoana împuternicită inițială[57].

64. Comitetul reamintește că, dacă un subcontractant nu își îndeplinește obligațiile, responsabilitatea finală pentru îndeplinirea obligațiilor acestui alt subcontractant revine operatorului. Persoana împuternicită inițială va rămâne răspunzătoare în fața operatorului, pentru ca operatorul să aibă posibilitatea de a formula o cerere contractuală împotriva persoanei împuternicite inițiale în cazul în care aceasta nu transmite aceleași obligații de protecție a datelor în contractele de subcontractare a serviciilor de prelucrare a datelor.

65. Persoanele împuternicite de operatori au obligația de a pune la dispoziția operatorului toate informațiile necesare pentru a demonstra conformitatea cu articolul 28 alineatul (3) litera (h) din RGPD. Prin urmare, la cererea operatorului, persoana împuternicită inițială va trebui să furnizeze contractele de subcontractare a serviciilor de prelucrare a datelor dintre persoana împuternicită inițială și persoanele împuternicite suplimentare.

66. În acest sens, clauzele contractuale standard („CCS-uri") operator-persoană împuternicită de operator ale Comisiei Europene[58] și CCS-urile pentru transferul internațional[59] oferă operatorului posibilitatea

[56] În Avizul comun CEPD - AEPD 2/2021 referitor la Decizia de punere în aplicare a Comisiei Europene privind clauzele contractuale standard pentru transferul de date cu caracter personal către țări terțe, CEPD și AEPD au subliniat că cerința prevăzută la articolul 28 alineatul (4) din RGPD trebuie luată în considerare de părțile implicate într-o relație de la persoană împuternicită de operator la persoană împuternicită de operator (punctul 66).

[57] Orientările CEPD nr. 7/2020, punctul 160: *„Impunerea „acelorași" obligații trebuie interpretată într-o manieră mai mult funcțională decât formală: nu este necesar ca în contract să se includă exact aceleași cuvinte ca cele utilizate în contractul dintre operator și persoana împuternicită de operator, ci trebuie să se asigure că obligațiile sunt aceleași în ceea ce privește substanța"* CEPD remarcă, de asemenea, că, atunci când două persoane împuternicite de operator se bazează pe modulul trei (persoană împuternicită de operator – persoană împuternicită de operator) din CCS-urile CE pentru transferul internațional, o garanție suplimentară este furnizată de persoana împuternicită inițială. În temeiul clauzei 8.1.d din CCS-urile CE pentru transferul internațional, exportatorul de date (persoana împuternicită inițială) garantează că a impus importatorului de date (subcontractantului) aceleași obligații în materie de protecție a datelor ca cele prevăzute în contractul sau în alt act juridic în temeiul dreptului Uniunii sau al statului membru între operator și exportatorul de date.

[58] În secțiunea 7 privind utilizarea de subcontractanți, articolul 7 alineatul (7) litera (c) din CCS-urile CE operator-persoană împuternicită de operator prevede: *„La cererea operatorului, persoana împuternicită de operator îi furnizează operatorului o copie a acestui contract de subcontractare și a oricăror modificări ulterioare. În măsura în care acest lucru este necesar pentru a proteja secretul de afaceri sau alte informații confidențiale, inclusiv date cu caracter personal, persoana împuternicită de operator poate să mascheze textul contractului înainte de a transmite copia*". Decizia de punere în aplicare (UE) 2021/915 a Comisiei din 4 iunie 2021 privind clauzele contractuale standard dintre operatori și persoanele împuternicite de operatori prevăzute la articolul 28 alineatul (7) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului și la articolul 29 alineatul (7) din Regulamentul (UE) 2018/1725 („CCS-urile CE operator-persoană împuternicită de operator").

[59] Modulul doi (operator-persoană împuternicită de operator), clauza 9 litera (c) din CCS-urile CE pentru transferul internațional prevede: *„Importatorul de date furnizează, la cererea exportatorului de date sau a operatorului, o copie a acestui contract de subcontractare și a oricăror modificări ulterioare. În măsura în care acest lucru este necesar pentru a proteja secretele de afaceri sau alte informații confidențiale, inclusiv date cu caracter personal, importatorul de date poate să mascheze textul contractului înainte de a transmite o copie."* În plus, modulul trei (operator-persoană împuternicită de operator) prevede că *„Importatorul de date furnizează, la cererea exportatorului de date sau a operatorului, o copie a acestui contract de subcontractare și a oricăror*

de a solicita o copie a contractului de subcontractare a serviciilor de prelucrare a datelor încheiat între persoana împuternicită inițială și persoanele împuternicite suplimentare. Această posibilitate este prevăzută și de cele trei CCS-uri operator-persoană împuternicită de operator adoptate de AS[60]. Această posibilitate este o expresie a dreptului de audit al operatorului în temeiul articolului 28 alineatul (3) litera (h) din RGPD. La cererea operatorului, persoana împuternicită de operator trebuie să furnizeze o astfel de copie.

67. CEPD observă însă că CCS-urile nu reglementează dacă un operator *trebuie* să solicite o asemenea copie pentru a respecta articolul 28 alineatul (1) din RGPD.

68. În acest sens, dacă operatorul alege sau nu să solicite o astfel de copie nu poate determina responsabilitatea operatorului. De asemenea, persoana împuternicită de operator are, în orice caz, obligații legale și contractuale de a impune aceleași obligații de protecție a datelor ca în contractul inițial.

69. Acestea fiind spuse, **operatorul nu are obligația de a solicita sistematic contractele de subcontractare a serviciilor de prelucrare a datelor pentru a verifica dacă obligațiile de protecție a datelor prevăzute în contractul inițial au fost transmise de-a lungul lanțului de prelucrare**. Operatorul trebuie să evalueze, de la caz la caz, dacă solicitarea unei copii a acestor contracte sau revizuirea lor oricând este necesară pentru a putea demonstra conformitatea în lumina principiului responsabilității. În contextul exercitării dreptului său de audit în temeiul articolului 28 alineatul (3) litera (h), operatorul trebuie să dispună de un proces de desfășurare a campaniilor de audit pentru a controla prin eșantionare dacă contractele cu subcontractanții săi conțin obligațiile necesare în materie de protecție a datelor.

70. Prin urmare, nevoia de a solicita o copie a contractului de subcontractare a serviciilor de prelucrare a datelor depinde de circumstanțele cazului. De exemplu, în caz de îndoieli cu privire la respectarea de către persoana împuternicită de operator sau de către subcontractant a cerințelor articolului 28 alineatele (1) și (4) sau la cererea AS, operatorul trebuie să solicite revizuirea contractului (de exemplu, în cazul în care persoana împuternicită suplimentară este afectată de o încălcare a securității datelor sau în cazul altor informații accesibile publicului sau al altor informații aflate la dispoziția operatorului); de exemplu, pot exista modele ale contractului de prelucrare a datelor al subcontractantului care nu îndeplinesc cerințele articolului 28 alineatul (3) din RGPD.

71. Pentru a asigura conformitatea cu articolul 28 alineatul (1) în lumina principiului responsabilității, o copie a contractelor de subcontractare a serviciilor de prelucrare a datelor poate ajuta operatorul să demonstreze că persoanele împuternicite de operator și subcontractanții lor prezintă garanții suficiente, inclusiv că persoana împuternicită de operator respectă articolul 28 alineatul (4) din RGPD. CEPD observă că este posibil ca un operator să nu fie în măsură să evalueze dacă garanțiile oferite în legătură cu un subcontractant sunt suficiente sau nu fără a accesa și evalua conținutul contractului de subcontractare. Deși garanțiile pot fi prevăzute în scris în contract, clauzele contractuale nu pot demonstra - prin ele însele - că garanțiile suficiente sunt efectiv puse în aplicare de părțile la contract.

---

modificări ulterioare. În măsura în care acest lucru este necesar pentru a proteja secretele de afaceri sau alte informații confidențiale, inclusiv date cu caracter personal, importatorul de date poate să mascheze textul contractului înainte de a transmite o copie." Decizia de punere în aplicare (UE) 2021/914 a Comisiei din 4 iunie 2021 privind clauzele contractuale standard pentru transferul de date cu caracter personal către țări terțe în temeiul Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului (JO L 199, 7.6.2021, p. 31).

[60] Clauzele contractuale standard ale AS DK în scopul respectării articolului 28 din RGPD, în special clauza 7.5; Clauzele contractuale standard ale AS LT în scopul respectării articolului 28 din RGPD, în special clauza 18; Clauzele contractuale standard ale AS SI în scopul respectării articolului 28 din RGPD, în special clauza 6.5.

2.2 Cu privire la interpretarea articolului 28 alineatul (1) din RGPD coroborat cu articolul 44 din RGPD (transferuri în lanțul de prelucrare - întrebările 1.2 și 1.3)

72. Întrebarea 1.2 din cerere urmărește să aducă clarificări în cazurile de transferuri sau de transferuri ulterioare de la o persoană împuternicită de operator (subcontractant) la altă persoană împuternicită de operator (subcontractant), în ce măsură operatorul, ca parte a obligației care îi revine în temeiul articolului 28 alineatul (1) din RGPD, coroborat cu articolul 44 din RGPD, ar trebui să evalueze documentația persoanelor împuternicite de operator (subcontractanților) conform căreia nivelul de protecție a datelor cu caracter personal nu este subminat de transferurile inițiale sau ulterioare.

73. Întrebarea 1.3 urmărește să aducă clarificări cu privire la măsura în care amploarea obligațiilor prevăzute la articolul 28 alineatul (1) din RGPD, coroborat cu articolul 5 alineatul (2) și cu articolul 24 din RGPD, astfel cum s-a răspuns la întrebarea 1.2, variază în funcție de riscul asociat activității de prelucrare. În caz afirmativ, AS DK a solicitat să știe care este amploarea acestor obligații pentru activitățile de prelucrare „cu risc scăzut” și „cu risc ridicat”.

Clarificări introductive

74. Din motive de claritate, în contextul prezentului aviz sunt furnizate câteva clarificări introductive referitoare la aceste întrebări.

75. În primul rând, CEPD înțelege termenul „transfer" în sensul prevăzut în Orientările CEPD nr. 5/2021 privind interacțiunea dintre articolul 3 și capitolul V din RGPD[61] [denumite în continuare „Orientările CEPD nr. 5/2021 (interacțiunea)"], care fac trimitere și la Orientările CEPD nr. 3/2018 privind domeniul de aplicare teritorială al RGPD[62]. După cum a subliniat anterior CEPD, accesul de la distanță dintr-o țară terță constituie un transfer dacă îndeplinește criteriile stabilite în Orientările CEPD nr. 5/2021 (interacțiunea)[63]. În orice caz, existența unui transfer declanșează aplicarea capitolului V din RGPD.

76. În al doilea rând, întrucât întrebarea 1.2 se referă la o situație în care o persoană împuternicită de operator sau un subcontractant efectuează un transfer inițial sau ulterior către altă persoană împuternicită de operator sau subcontractant, operatorul nu este exportatorul de date; ci exportatorul de date este o persoană împuternicită de operator, care transferă datele cu caracter personal altei persoane împuternicite de operator de-a lungul lanțului în numele operatorului, și nu unui operator separat. Se exclud, prin urmare, datele cu caracter personal transferate către operatori separați, și anume tribunale, instanțe sau autorități administrative din țări terțe. Prin urmare, interpretarea articolului 48 din RGPD nu intră în domeniul de aplicare al acestor întrebări.

77. În al treilea rând, CEPD observă că întrebarea 1.2 se referă la transferurile care au loc de-a lungul lanțului de prelucrare în conformitate cu instrucțiunile documentate ale operatorului în temeiul articolului 28 alineatul (3) litera (a) din RGPD. Trebuie subliniat că este la latitudinea operatorului să decidă dacă un transfer de date cu caracter personal în afara SEE este posibil ca parte a activităților de prelucrare încredințate persoanei împuternicite de operator (subcontractanților). Persoana împuternicită de operator ar trebui să se abțină de la efectuarea oricărui transfer inițial sau ulterior în afara instrucțiunilor operatorului[64]. Instrucțiunile documentate ale operatorului cu privire la transferurile inițiale sau ulterioare de date cu caracter personal trebuie transmise de-a lungul lanțului de prelucrare[65].

78. În al patrulea rând, CEPD precizează că noțiunea de risc menționată în întrebarea 1.3 trebuie înțeleasă ca fiind riscul pentru drepturile și libertățile persoanelor vizate ale căror date cu caracter personal sunt prelucrate, în sensul considerentelor 75 și 76 din RGPD (după cum se menționează la punctul 35 de mai sus).

[61] Orientările CEPD nr. 5/2021 privind interacțiunea dintre aplicarea articolului 3 și dispozițiile referitoare la transferurile internaționale în conformitate cu capitolul V din RGPD, versiunea 2.0, adoptate la 14 februarie 2023, în care punctul 9 stabilește cele trei criterii cumulative pentru a califica o operațiune de prelucrare ca transfer și, mai general, secțiunea 2 detaliază aceste criterii.

[62] Orientările CEPD nr. 5/2021 (interacțiunea), punctul 12, cu trimitere la Orientările CEPD nr. 3/2018 privind domeniul de aplicare teritorială al RGPD, versiunea 2.1, adoptate la 12 noiembrie 2019 (cu rectificarea din 7 ianuarie 2020), pagina 5 și secțiunile 1-3. Vezi în special litera „(d) Persoană împuternicită de operator nestabilită în Uniune" de la secțiunea 2.

[63] Orientările CEPD nr. 5/2021 (interacțiunea), punctul 16.

[64] Articolul 29 din RGPD. După cum a reamintit CEPD, „*Contractul trebuie să precizeze cerințele pentru transferurile către țări terțe sau către organizații internaționale, ținând seama de dispozițiile capitolului V din RGPD*" (Orientările CEPD nr. 7/2020, punctul 119). De exemplu, operatorul poate alege să interzică transferurile sau să le permită numai către anumite țări.

[65] Articolul 28 alineatul (4) din RGPD.

Responsabilitatea operatorului există chiar dacă persoanele împuternicite de operator (subcontractanții) efectuează transferurile inițiale sau ulterioare

79. În ceea ce privește fondul cererii, CEPD a precizat deja că *„(...) va exista o situație de transfer în care o persoană împuternicită de operator [fie în temeiul articolului 3 alineatul (1), fie în temeiul articolului 3 alineatul (2) pentru o anumită prelucrare (...)] trimite date unei alte persoane împuternicite de operator sau chiar unui operator dintr-o țară terță, conform instrucțiunilor operatorului său. În aceste cazuri, persoana împuternicită de operator acționează în calitate de exportator de date în numele operatorului și trebuie să se asigure că dispozițiile capitolului V sunt respectate pentru transferul în cauză în conformitate cu instrucțiunile operatorului, inclusiv că este utilizat un instrument de transfer adecvat. Având în vedere că transferul este o activitate de prelucrare efectuată în numele operatorului,* ***operatorul este, de asemenea, responsabil și ar putea fi tras la răspundere în temeiul capitolului V și, de asemenea, trebuie să se asigure că persoana împuternicită de operator oferă garanții suficiente în temeiul articolului 28****."*[66]

80. Cu alte cuvinte, în cazul unui transfer, chiar dacă nu este efectuat direct de operator, ci de o persoană împuternicită de operator în numele operatorului, operatorul este în continuare supus obligațiilor care decurg atât din articolul 44 din RGPD, cât și din articolul 28 alineatul (1) din RGPD[67] [68].

Responsabilitatea care decurge din articolul 44 din RGPD

81. Obligațiile prevăzute la articolul 44 din RGPD[69] se adresează atât persoanelor împuternicite de operator (în contextul avizului, acționând ca exportatori de date), cât și operatorilor[70]. Prin urmare, atât persoanele împuternicite de operatori, cât și operatorii trebuie să se asigure că nivelul de protecție a datelor cu caracter personal nu este subminat de transferul inițial sau ulterior, indiferent de motivul transferului[71]. De exemplu, atât operatorul, cât și persoana împuternicită de operator rămân, în principiu, responsabili, în temeiul capitolului V din RGPD, pentru un transfer inițial sau ulterior ilegal[72] și, prin urmare, ar putea fi trași la răspundere atât împreună, cât și individual în cazul unei încălcări.

Responsabilitatea care decurge din articolul 28 alineatul (1) din RGPD

82. În temeiul principiului responsabilității, operatorii sunt obligați să ia „măsurile corespunzătoare" pentru a preveni orice încălcare a normelor prevăzute în RGPD pentru a asigura dreptul la protecția

---

Orientările[66] CEPD nr. 5/2021 (interacțiunea), punctul 19, sublinierea este adăugată cu caractere aldine.

[67] De asemenea, este relevant să se precizeze că articolul 28 alineatul (1) din RGPD se referă la îndeplinirea cerințelor din RGPD și, prin urmare, trebuie interpretat ca incluzând dispozițiile capitolului V referitoare la transferurile inițiale sau ulterioare de date cu caracter personal către țări terțe. Aceasta acoperă atât transferurile inițiale, cât și transferurile ulterioare, vezi articolul 44 din RGPD.

[68] În sensul acestei secțiuni a avizului, sunt abordate obligațiile care decurg din articolul 44 și din articolul 28 alineatul (1) din RGPD, precizându-se că operatorul este în continuare supus tuturor obligațiilor aplicabile operatorilor în temeiul RGPD.

[69] Articolul 44 din RGPD trimite la dispozițiile capitolului V din RGPD.

[70] Articolul 44 din RGPD abordează atât „operatorul, cât și persoana împuternicită de operator" pentru respectarea capitolului V; vezi și considerentul 101. Din acest motiv, Recomandările nr. 1/2020 ale CEPD privind măsurile care completează instrumentele de transfer pentru a asigura conformitatea cu nivelul UE de protecție a datelor cu caracter personal, versiunea 2.0, adoptată la 18 iunie 2021 (denumite în continuare „Recomandările CEPD nr. 1/2020") se aplică „exportatorilor de date" [operatori sau persoane împuternicite de operatori (subcontractanți) care prelucrează date cu caracter personal].

[71] Hotărârea CJUE din 16 iulie 2020, *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems*, (denumită în continuare „Hotărârea CJEU Schrems II') cauza C-311/18, ECLI:EU:C:2020:559, punctul 92.

[72] Operatorul poate solicita înapoi de la persoana împuternicită de operator compensația care corespunde părții sale de responsabilitate, sub rezerva îndeplinirii condițiilor prevăzute la articolul 82 alineatul (5) din RGPD.

datelor[73] și acest lucru include prevenirea încălcării capitolului V din RGPD. Această responsabilitate se aplică înainte de începerea transferului și atâta timp cât datele cu caracter personal transferate sunt prelucrate în țara terță.

83. După cum s-a explicat mai sus la punctele 47-48, *obligația operatorului* de a verifica dacă persoanele împuternicite de operator (subcontractanții) prezintă garanții suficiente pentru punerea în aplicare a măsurilor stabilite de operator în temeiul articolului 28 alineatul (1) din RGPD[74] trebuie să se aplice indiferent de riscul pentru drepturile și libertățile persoanelor vizate. *Amploarea* acestei verificări va varia însă în practică în funcție de natura măsurilor organizatorice și tehnice stabilite de operator pe baza, printre alte criterii, a riscului asociat prelucrării[75]. În această privință, existența unui transfer inițial sau ulterior către țări terțe de-a lungul lanțului de prelucrare poate mări riscurile care decurg din prelucrare și, prin urmare, poate avea un impact asupra măsurilor „adecvate" stabilite de operator[76].

84. La cerere, operatorul – asistat de persoana împuternicită de operator și de subcontractanți – ar trebui să poată demonstra autorității de supraveghere competente conformitatea sa cu cerințele prevăzute la articolul 28 alineatul (1) din RGPD. Documentația adecvată s-ar putea baza - printre altele - pe informațiile primite de la persoanele împuternicite de operator în contextul angajării persoanelor împuternicite de operator (subcontractanților) [77] (vezi punctele 54-56), dar și cu asistența persoanelor împuternicite de operator, în conformitate cu articolul 28 alineatul (3) litera (h) din RGPD (vezi punctele 51-52).

85. Operatorul are nevoie, de asemenea, de toate informațiile relevante pentru a emite instrucțiunile necesare pentru a transfera datele cu caracter personal către țările terțe respective și pentru a putea respecta principiul responsabilității prevăzut la articolul 5 alineatul (2) și articolul 24 din RGPD, precum și dispozițiile articolului 28 alineatul (1), ale articolului 32 și ale capitolului V din RGPD[78]. Operatorul poate obiecta sau poate să nu autorizeze angajarea unei persoane împuternicite suplimentare în cazul în care aceasta ar implica un transfer de date cu caracter personal de la persoana împuternicită inițială

[73] Vezi secțiunea de mai sus privind articolul 5 alineatul (2) și articolul 24 alineatul (1), combinată cu articolul 28 alineatul (1) din RGPD.

[74] Pentru a evita orice îndoială, trebuie precizat că „măsurile tehnice și organizatorice adecvate" menționate la articolul 24 alineatul (1) și 28 alineatul (1) din RGPD nu trebuie confundate cu „măsurile suplimentare", menționate în Recomandările CEPD nr. 1/2020 (punctul 50: *„Măsurile suplimentare" sunt, prin definiție, suplimentare față de garanțiile pe care instrumentul de transfer prevăzut la articolul 46 din RGPD le oferă deja și față de orice alte cerințe de securitate aplicabile (de exemplu, măsuri tehnice de securitate) stabilite în RGPD*", făcând trimitere la considerentul 109 din RGPD și hotărârea CJUE Schrems II, punctul 133).

[75] Vezi definiția riscului, așa cum este explicată la punctele 35 și 78.

[76] Considerentul 116 din RGPD prevede: *„Fluxul transfrontalier de date cu caracter personal în afara Uniunii poate expune unui risc sporit capacitatea persoanelor fizice de a-și exercita drepturile în materie de protecție a datelor, în special pentru a-și asigura protecția împotriva utilizării sau a divulgării ilegale a acestor informații."*

[77] Vezi și clauza 9 litera (a) din modulul trei (persoană împuternicită de operator - persoană împuternicită de operator) din CCS-urile CE pentru transferul internațional și anexa III la acestea; vezi și clauza 9 litera (a) din modulul doi (operator-persoană împuternicită de operator); și clauza 7.7 litera (a) din CCS-urile CE (operator-persoană împuternicită de operator) și anexa IV la acestea „Lista subcontractanților". Atât anexa II la CCS CE pentru transfer internațional, cât și anexa IV la CCS CE operator-persoană împuternicită de operator trebuie completate cu următoarele informații privind subcontractanții în cazul unei autorizații specifice din partea operatorului: numele, adresa, numele, funcția și datele de contact ale persoanei de contact, precum și descrierea prelucrării. În plus, secțiunea B „Descrierea transferului" din anexa I la CCS-urile CE pentru transferul internațional include „Pentru transferurile către persoane împuternicite de operatori (subcontractanți), a se preciza, de asemenea, obiectul, natura și durata prelucrării". În mod similar, anexa II la CCS-urile operator-persoană împuternicită de operator include „Pentru prelucrarea de către persoane împuternicite de operator (subcontractanți), a se specifica și obiectul, natura și durata prelucrării".

[78] Orientările CEPD nr. 7/2020, punctul 152, nota de subsol 69.

(în calitate de exportator) către persoana împuternicită suplimentară avută în vedere (în calitate de importator) pe baza informațiilor primite.

86. Conform punctului 58 de mai sus, operatorul este responsabil în ultimă instanță pentru orice încălcare a articolului 28 alineatul (1) din RGPD în ceea ce privește utilizarea de persoane împuternicite de operatori (subcontractanți) și poate fi tras la răspundere în acest sens. CEPD subliniază că dificultățile practice invocate de operatori în ceea ce privește controlul implicării subcontractanților de către persoana împuternicită de operator – ceea ce le poate îngreuna verificarea „garanțiilor suficiente", în special în ceea ce privește transferurile către țări terțe – nu exonerează operatorul de responsabilitățile sale în materie de prelucrare[79].

87. Mai jos sunt descrise exemple neexhaustive de documente pe care operatorul trebuie să le evalueze și să fie în măsură să le prezinte autorității de supraveghere competente – cartografierea transferului, motivul transferului utilizat și, după caz, „evaluarea impactului transferului" și măsurile suplimentare.

Cartografierea transferurilor:

88. Ca prim pas, când datele cu caracter personal vor fi transferate către țări terțe în legătură cu utilizarea de persoane împuternicite de operator (subcontractanți), operatorul trebuie să evalueze și să poată prezenta documentația referitoare la cartografierea transferului[80]. Operatorul trebuie să se asigure că exportatorul (care prelucrează date cu caracter personal în numele său) realizează o cartografiere a transferului, stabilind ce date cu caracter personal sunt transferate (inclusiv accesul la distanță), unde și în ce scopuri[81]. Operatorul se poate baza pe această cartografiere și, dacă este necesar, o poate dezvolta. De exemplu, în cazul în care cartografierea primită de operator pare incompletă[82], inexactă sau ridică întrebări, operatorul trebuie să solicite informații suplimentare, să verifice informațiile și să le completeze/să le corecteze, dacă este necesar.

89. Operatorul trebuie să primească aceste informații[83] înainte de angajarea unei persoane împuternicite suplimentare. De asemenea, trebuie reamintit că operatorul este supus unor cerințe specifice de transparență în ceea ce privește transferurile către țări terțe în temeiul articolului 13 alineatul (1) litera (f), al articolului 14 alineatul (1) litera (f), al articolului 15 alineatul (1) litera (c) și al articolului 15 alineatul (2) din RGPD, precum și cerinței de a ține evidența activităților de prelucrare în temeiul articolului 30 alineatul (1) literele (d) și (e) din RGPD. Pentru a îndeplini aceste cerințe, operatorul trebuie să știe unde se află subcontractanții și unde au loc transferurile, inclusiv accesul de la distanță[84].

[79] Raportul MIE privind serviciile de cloud, p. 16.

[80] „Cartografierea" se referă la primul pas (așa-numitul „Cunoașterea transferurilor dumneavoastră") din Recomandările nr. 1/2020 ale CEPD, secțiunea 2.1 „Pasul 1: Cunoașterea transferurilor dumneavoastră" Acest prim pas se aplică indiferent de motivul transferului.

[81] Trebuie precizat că scopurile sunt stabilite de operator, împreună cu „mijloacele esențiale" ale prelucrării (vezi Orientările CEPD nr. 7/2020, punctul 40).

[82] De exemplu, dacă cartografierea nu specifică locația subcontractanților sau dacă transferurile sub formă de acces de la distanță nu sunt menționate în cartografiere atunci când au loc.

[83] După cum s-a explicat mai sus la punctele 54-56.

[84] Cartografierea este necesară și când părțile completează anexele relevante la CCS-urile CE pentru transferul internațional și la CCS-urile CE operator-persoană împuternicită de operator (vezi nota de subsol 80 de mai sus).

Motivul pentru transfer utilizat și, dacă este cazul, „evaluarea impactului transferului” și măsurile suplimentare:

90. Operatorul trebuie să evalueze și să poată prezenta documentația referitoare la motivul transferului[85] pe care exportatorul se bazează în conformitate cu instrucțiunile operatorului[86]. Asta înseamnă că operatorul trebuie să primească aceste informații de la persoanele împuternicite de operator (subcontractanți)/exportatori înainte ca transferurile să aibă loc. CEPD a reamintit, în acest context, că operatorul este supus unor cerințe specifice de transparență în ceea ce privește „existența sau absența unei decizii privind caracterul adecvat al nivelului de protecție” în temeiul articolului 45 din RGPD sau a „garanțiilor adecvate” prevăzute în conformitate cu articolul 46 din RGPD [articolul 13 alineatul (1) litera (f), articolul 14 alineatul (1) litera (f) și articolul 15 alineatul (2) din RGPD[87]].

91. În ceea ce privește sfera de aplicare a obligației operatorului de a evalua această documentație, aceasta depinde de tipul de motiv utilizat pentru transferul inițial sau ulterior de către persoanele împuternicite de operator (subcontractanți) (ca exportator de date)[88]:

92. Transferurile pot fi efectuate pe baza unei **decizii privind caracterul adecvat** al nivelului de protecție dacă, în temeiul articolului 45 din RGPD, Comisia a decis că o țară terță, un teritoriu terț sau unul sau mai multe sectoare specificate din țara terță respectivă sau o organizație internațională asigură un nivel adecvat de protecție. Pentru a evalua dacă nivelul de protecție este adecvat, Comisia ia în considerare – printre alte criterii – normele privind transferul ulterior de date cu caracter personal către altă țară terță sau organizație internațională care sunt respectate în țara sau organizația internațională respectivă, jurisprudența, precum și drepturile efective și opozabile ale persoanelor vizate și căi de atac administrative și judiciare eficace pentru persoanele vizate ale căror date cu caracter personal sunt transferate[89].

93. În acest context, când un transfer este efectuat de o persoană împuternicită de operator (subcontractant) (în numele operatorului) pe baza unei decizii privind caracterul adecvat al nivelului de protecție în temeiul articolului 45 din RGPD, gradul de verificare solicitat operatorului în temeiul articolului 28 alineatul (1) din RGPD ca persoana împuternicită de operator (subcontractantul) să prezinte garanții suficiente în ceea ce privește conformitatea cu capitolul V din RGPD trebuie să acopere următoarele elemente:

[85] Recomandările CEPD nr. 1/2020, secțiunea 2.2. „Pasul 2: Identificarea instrumentelor de transfer pe care vă bazați”

[86] Articolul 28 alineatul (3) litera (a) din RGPD.

[87] Orientările CEPD nr. 1/2022 (dreptul de acces), punctul 122.

[88] În conformitate cu instrucțiunile documentate ale operatorului cu privire la transferurile de date cu caracter personal de-a lungul lanțului de prelucrare.

[89] Vezi articolul 45 din RGPD și Criteriile de referință privind caracterul adecvat al nivelului de protecție, adoptate la 28 noiembrie 2017, WP254, aprobate de CEPD la 25 mai 2018, pagina 7: „*Transferurile suplimentare de date cu caracter personal efectuate de destinatarul inițial al transferului inițial de date ar trebui permis doar atunci când destinatarul ulterior (adică destinatarul transferului ulterior) este supus tot unor norme (inclusiv normelor contractuale) care acordă un nivel adecvat de protecție și respectă instrucțiunile relevante atunci când prelucrează date în numele operatorului de date. Nivelul de protecție al persoanelor fizice ale căror date sunt transferate nu trebuie să fie subminat de transferul ulterior. Destinatarul inițial al datelor transferate din UE este responsabil să asigure faptul că sunt prevăzute garanții adecvate pentru transferurile ulterioare de date în absența unei decizii privind caracterul adecvat al nivelului de protecție. Astfel de transferuri ulterioare de date ar trebui să aibă loc numai în scopuri limitate și specificate și atâta timp cât există un temei juridic pentru prelucrarea respectivă*”.

- dacă decizia privind caracterul adecvat al nivelului de protecție este în vigoare[90];

- și dacă transferurile efectuate în numele operatorului intră în domeniul de aplicare al unei astfel de decizii (de exemplu, categoriile de date cu caracter personal sau sectoarele care intră în domeniul de aplicare)[91].

94. În cazul în care datele cu caracter personal transferate de o persoană împuternicită de operator (subcontractant) (în numele operatorului) pe baza unei decizii privind caracterul adecvat al nivelului de protecție fac obiectul unui **transfer ulterior** din țara terță respectivă, nivelul de protecție a persoanelor fizice garantat de RGPD pentru un astfel de transfer ulterior nu trebuie, de asemenea, să fie subminat[92]. În acest sens, conform articolului 45 alineatul (2) litera (a) din RGPD, orice decizie privind caracterul adecvat al nivelului de protecție emisă de Comisia Europeană acoperă, printre altele, normele țărilor terțe care reglementează transferurile ulterioare. Prin urmare, în temeiul articolului 44 din RGPD, operatorul nu trebuie să verifice aceste cerințe pe cont propriu.

95. În ceea ce privește obligația care îi revine operatorului în temeiul articolului 28 alineatul (1) din RGPD, asta înseamnă că operatorul ar trebui să se asigure că persoana împuternicită de operator (subcontractantul) oferă „garanții suficiente" și în ceea ce privește transferurile ulterioare efectuate de o persoană împuternicită de un operator (subcontractant) dintr-o țară adecvată.

96. În lipsa unei decizii privind caracterul adecvat, transferurile pot fi efectuate sub rezerva furnizării de „**garanții adecvate**" conform **articolului 46 din RGPD**. În acest caz, operatorul trebuie să evalueze garanțiile adecvate puse în aplicare și să fie atent la orice legislație problematică care ar putea împiedica subcontractantul să respecte obligațiile stabilite în contractul său cu persoana împuternicită inițială[93]. Mai precis, operatorul trebuie să se asigure că se efectuează o astfel de „evaluare a impactului transferului"[94], conform jurisprudenței[95] și după cum se explică în Recomandările CEPD nr. 1/2020. Documentația referitoare la garanțiile adecvate instituite, la „evaluarea impactului transferului" și la posibilele măsuri suplimentare trebuie elaborată de operator/exportator[96] (dacă este cazul, în colaborare cu persoana împuternicită de operator/importatorul[97]). Operatorul se poate baza pe evaluarea pregătită de persoana împuternicită de operator (subcontractant) și, dacă este nevoie, o

[90] Recomandările CEPD nr. 1/2020, punctul 19: „*Dacă [dvs., exportatorul de date] 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 trebuie să luați alte măsuri, astfel cum se descrie în prezentele recomandări. 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*."

[91] Recomandările CEPD nr. 1/2020, punctul 19.

[92] Vezi articolul 44 din RGPD: „*condițiile prevăzute în prezentul capitol sunt respectate (...), inclusiv în ceea ce privește transferurile ulterioare de date cu caracter personal din țara terță sau de la organizația internațională către o altă țară terță sau către o altă organizație internațională*".

[93] În această privință, vezi hotărârea CJUE în cauza Schrems II, punctele 132 și 133, în care CJUE subliniază natura contractuală a CCS-urilor CE pentru transfer internațional.

[94] Această evaluare este explicată mai detaliat în Recomandările CEPD nr. 1/2020, pasul 3 intitulat „Evaluarea eficacității instrumentului de transfer prevăzut la articolul 46 din RGPD pe care vă bazați având în vedere toate circumstanțele transferului".

[95] Hotărârea CJUE Schrems II, punctul 134.

[96] Recomandările nr. 1/2022 privind cererea de aprobare și elementele și principiile care trebuie să se regăsească în regulile corporatiste obligatorii pentru operatori (articolul 47 din RGPD) adoptate la 20 iunie 2023, versiunea 2.1, punctul 10: „(...) *este, de exemplu, responsabilitatea fiecărui exportator de date să evalueze, pentru fiecare transfer, de la caz la caz, dacă este necesar să pună în aplicare măsuri suplimentare pentru a asigura un nivel de protecție echivalent în esență cu cel prevăzut de RGPD*."

[97] În hotărârea CJUE Schrems II, punctul 134, CJUE a remarcat că un astfel de exercițiu de verificare poate fi efectuat în colaborare cu importatorul, după caz. Vezi și Recomandările CEPD nr. 1/2020, secțiunea 4.

poate dezvolta. De exemplu, dacă evaluarea primită de operator pare incompletă, inexactă sau ridică semne de întrebare, operatorul trebuie să solicite informații suplimentare, să verifice informațiile și să le completeze/corecteze dacă este nevoie, ținând cont de faptul că evaluarea trebuie să fie în conformitate cu Recomandările CEPD nr. 1/2020 și cu etapele stabilite în ele[98]. Acest lucru include identificarea legilor și practicilor relevante având în vedere toate circumstanțele transferului[99] și identificarea măsurilor suplimentare adecvate, dacă este necesar[100]. În această privință, operatorul trebuie să acorde o atenție deosebită măsurii în care exportatorul de date, și anume persoana împuternicită de operator sau subcontractantul, a evaluat dacă există elemente în legislația și/sau practicile din țara terță care ar putea afecta eficacitatea garanțiilor adecvate ale motivului pentru transfer pe care exportatorul se bazează[101], în special datorită legislației și practicilor care reglementează accesul la datele cu caracter personal transferate de autoritățile publice din țara terță[102].

97. În plus și în mod similar cu transferurile bazate pe o decizie privind caracterul adecvat (articolul 45 din RGPD, vezi punctele 94 și 95 de mai sus), când datele cu caracter personal sunt transferate de o persoană împuternicită de operator (subcontractant) pe baza unor garanții adecvate în temeiul articolului 46 din RGPD, obligația operatorului în temeiul articolului 28 alineatul (1) din RGPD acoperă și obligația de a se asigura că persoana împuternicită de operator (subcontractantul) prezintă garanții suficiente în ceea ce privește **transferurile ulterioare**. Garanțiile adecvate prevăzute la articolul 46 din RGPD includ, de obicei, dispoziții care stabilesc norme care vor reglementa transferurile ulterioare[103]. Asta înseamnă că operatorii nu trebuie să verifice dacă normele respective sunt, ca atare, conforme cu cerințele din capitolul V din RGPD. Operatorii trebuie să fie însă în măsură să prezinte documente referitoare la aceste transferuri ulterioare. Asta înseamnă că operatorul trebuie să primească aceste informații de la persoanele împuternicite de operatori (subcontractanți)/exportatori, demonstrând că importatorii respectă efectiv condițiile pentru transferurile ulterioare, așa cum prevede instrumentul de garanții adecvat.

2.3 Cu privire la interpretarea articolului 28 alineatul (3) litera (a) din RGPD (întrebarea 2)

98. Pentru a asigura alocarea transparentă a responsabilităților și obligațiilor atât pe plan intern (între operatori și persoanele împuternicite de operator), cât și pe plan extern față de persoanele vizate și autoritățile de reglementare, conform articolului 28 alineatul (3) din RGPD, orice prelucrare a datelor

[98] Vezi, în special „Pasul 3: Evaluarea eficacității instrumentului de transfer prevăzut la articolul 46 din RGPD pe care vă bazați având în vedere toate circumstanțele transferului", Pasul 4: Adoptarea de măsuri suplimentare" și „Pasul 6: Reevaluarea la intervale corespunzătoare", așa cum se explică în Recomandările nr. 1/2020 ale CEPD.
[99] Hotărârea CJUE Schrems II, punctul 126. Vezi și Recomandările CEPD nr. 1/2020, secțiunea 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 și în special punctul 33. În hotărârea CJUE Schrems II, punctul 134, CJUE a menționat că un astfel de exercițiu de verificare poate fi realizat în colaborare cu importatorul, după caz (vezi și Recomandările CEPD nr. 1/2020, punctul 30).
[100] Pe baza jurisprudenței, este de competența operatorului sau a persoanei împuternicite de operator să verifice, de la caz la caz și, după caz, în colaborare cu destinatarul datelor, dacă legislația țării terțe de destinație asigură o protecție adecvată, în temeiul dreptului Uniunii, a datelor cu caracter personal transferate în temeiul clauzelor standard de protecție a datelor, oferind, dacă este necesar, garanții suplimentare față de cele oferite de clauzele respective (Hotărârea Schrems II a CJUE, punctul 134). Vezi și Recomandările CEPD nr. 1/2020, secțiunea 2.4., „Pasul 4: Adoptarea de măsuri suplimentare"
[101] Vezi Recomandările CEPD nr. 1/2020, secțiunea 2.3 („Pasul 3").
[102] Vezi Recomandările CEPD nr. 1/2020, punctul 41 și următoarele.
[103] Vezi, de exemplu, clauza 8.7 (modulul unu), respectiv 8.8 (modulele doi și trei) din CCS-urile CE pentru transfer (Decizia de punere în aplicare 2021/914 a Comisiei) din 4.6.2021.

cu caracter personal de către o persoană împuternicită de operator trebuie să fie reglementată printr-un contract sau alt act juridic în temeiul legislației UE sau al statului membru[104] între operator și persoana împuternicită de operator. Conform articolului 28 alineatul (3) litera (a) din RGPD, contractul stipulează, în particular că operatorul „*prelucrează datele cu caracter personal numai pe baza unor instrucțiuni susținute de documente din partea operatorului, inclusiv în ceea ce privește transferurile de date cu caracter personal către o țară terță sau o organizație internațională, cu excepția cazului în care această obligație îi revine în temeiul dreptului Uniunii sau al dreptului statului membru care i se aplică"*. Această dispoziție menționează și că „*în acest caz, persoana împuternicită de operator notifică această obligație juridică operatorului înainte de prelucrare, cu excepția cazului în care legislația respectivă interzice această informare din motive importante legate de interesul public*".

99. Cererea se referă la existența unor contracte care includ un angajament de a prelucra date cu caracter personal doar la instrucțiunile operatorului „*cu excepția cazului în care această obligație îi revine în temeiul legii sau al unei ordonanțe obligatorii a unui organism guvernamental*" (omițând trimiterea la dreptul Uniunii sau la dreptul intern). În acest sens, s-au trimis mai multe întrebări la CEPD, abordate împreună în secțiunea de mai jos:

> 2 Un contract sau alt act juridic în temeiul dreptului Uniunii sau al dreptului intern în temeiul articolului 28 alineatul (3) din RGPD trebuie să conțină excepția prevăzută la articolul 28 alineatul (3) litera (a), „*cu excepția cazului în care persoanei împuternicite de operator îi revine această obligație în temeiul dreptului Uniunii sau al dreptului intern care i se aplică*" (textual sau în termeni foarte similari) pentru a fi în conformitate cu RGPD?
>
> 2a Dacă răspunsul la întrebarea 2 este negativ, atunci când un contract sau alt act juridic în temeiul dreptului Uniunii sau al unui stat membru extinde excepția de la articolul 28 alineatul (3) litera (a) din RGPD pentru a acoperi și dreptul unei țări terțe (de exemplu „cu excepția cazului în care această obligație îi revine în temeiul legii sau al unei ordonanțe obligatorii a unui organism guvernamental"), este aceasta în sine o încălcare a articolului 28 alineatul (3) litera (a) din RGPD?

100. Orientările CEPD nr. 7/2020 reamintesc „*importanța negocierii și a redactării cu atenție a acordurilor privind prelucrarea datelor"* în ceea ce privește orice cerință legală a UE sau a unui stat membru la care se supune persoana împuternicită de operator[105]. Cât privește conținutul, Orientările CEPD nr. 7/2020 menționează că un acord „*între operator și persoana împuternicită de operator trebuie să respecte cerințele articolul 28 din RGPD pentru a asigura că persoana împuternicită de operator prelucrează date cu caracter personal cu respectarea RGPD*. *Orice astfel de acord trebuie să țină seama de responsabilitățile specifice ale operatorilor și ale persoanelor împuternicite de operatori. Deși articolul 28 prevede o listă de puncte care trebuie abordate în orice contract care reglementează relația dintre operatori și persoanele împuternicite de operatori, acesta permite negocieri între părțile la astfel de contracte*"[106]. Marja de negociere este limitată de cerințele prevăzute la articolul 28 alineatul (3) din RGPD.

[104] În continuare, termenul „**contract**" va fi folosit pentru a face referire la „un contract sau alt act juridic în temeiul dreptului UE sau al statului membru".
[105] Orientările CEPD nr. 7/2020, punctul 121.
[106] Orientările CEPD nr. 7/2020, punctul 109.

101. În primul rând, angajamentul persoanei împuternicite de operator de a prelucra datele cu caracter personal numai pe baza unor instrucțiuni documentate din partea operatorului este un element esențial al contractului.

102. Cu toate acestea, după cum recunoaște articolul 28 alineatul (3) litera (a) din RGPD, persoanele împuternicite de operatori pot prelucra în mod legal date cu caracter personal – altele decât pe baza unor instrucțiuni documentate ale operatorului – în scopul respectării obligațiilor legale prevăzute de legislația UE sau a statelor membre (denumită în continuare „**cerința legală a UE/SM**"). Aceeași dispoziție solicită și un angajament din partea persoanei împuternicite de operator de a informa operatorul - în prealabil - în cazul în care se aplică o cerință legală a UE/MS de a prelucra / transfera date cu caracter personal către o țară terță sau o organizație internațională, cu excepția cazului în care legea respectivă interzice o astfel de informare din motive importante de interes public. Acest angajament este inclus în mod explicit, cu o formulare foarte asemănătoare cu cea de la articolul 28 alineatul (3) litera (a) din RGPD, în CCS-urile CE operator-persoana împuternicită de operator[107] și în mai multe clauze contractuale standard, în special în CCS-urile adoptate de AS daneză[108], slovenă[109] și lituaniană[110] în scopul respectării articolului 28 din RGPD.

103. În afară de angajamentul de a prelucra numai pe bază de instrucțiuni documentate din partea operatorului, articolul 28 alineatul (3) litera (a) din RGPD conține, prin urmare, trei elemente principale: (a) o normă care reglementează situațiile în care o cerință legală obligă persoana

[107] Vezi, în special, clauzele 7.1 (a) și 7.8 (a):
- Clauza 7.1.a: „*Persoana împuternicită de operator prelucrează datele cu caracter personal numai pe baza unor instrucțiuni documentate din partea operatorului, cu excepția cazului în care persoanei împuternicite de operator îi revine această obligație în temeiul dreptului Uniunii sau al dreptului intern care i se aplică. În acest caz, persoana împuternicită de operator îl informează pe operator cu privire la respectiva obligație juridică înainte de prelucrare, cu excepția situației în care legislația interzice o astfel de informare din motive importante legate de interesul public. De asemenea, operatorul poate da instrucțiuni ulterioare pe întreaga durată a prelucrării datelor cu caracter personal. Aceste instrucțiuni trebuie să fie întotdeauna documentate*." (sublinierea noastră). În avizul lor comun privind proiectul de CCS CE, pentru a spori coerența, CEPD și AEPD au recomandat includerea formulării complete a articolului 28 alineatul (3) litera (a) (adăugând astfel o trimitere la obligația persoanei împuternicite de operator de a informa operatorul cu privire la cerința legală). Avizul comun nr. 1/2021 al CEPD și AEPD referitor la Decizia de punere în aplicare a Comisiei Europene privind clauzele contractuale standard dintre operatori și persoanele împuternicite de operatori referitoare la chestiunile prevăzute la articolul 28 alineatul (7) din Regulamentul (UE) 2016/679 și la articolul 29 alineatul (7) din Regulamentul (UE) 2018/1725, punctul 38. Formularea „*cu excepția cazului în care persoanei împuternicite de operator îi revine această obligație în temeiul dreptului Uniunii sau al dreptului intern care i se aplică*" era deja prezentă în proiectul de CCS-uri.
- Clauza 7.8.a: „*Orice transfer de date către o țară terță sau o organizație internațională realizat de persoana împuternicită de operator are loc pe baza instrucțiunilor documentate din partea operatorului sau pentru a îndeplini o cerință specifică în temeiul dreptului Uniunii sau al dreptului intern care i se aplică persoanei împuternicite de operator și se desfășoară în conformitate cu capitolul V din Regulamentul (UE) 2016/679 sau din Regulamentul (UE) 2018/1725*." În ceea ce privește clauza 7.8 litera (a), AEPD și CEPD au recomandat includerea unei trimiteri la posibilitatea ca persoana împuternicită de operator să efectueze transferuri pe baza unei cerințe specifice prevăzute de legislația Uniunii sau a statului membru la care este supusă persoana împuternicită de operator, care nu a fost specificată inițial în proiectele de CCS. Anexa 2 la Avizul comun nr. 1/2021 al CEPD-AEPD, Observații privind clauza 7.7 litera (a).

[108] Clauzele contractuale standard ale AS din daneză în scopul respectării articolului 28 din RGPD, în special clauzele 4.1 și 8.2. În Avizul CEPD nr. 14/2019 privind proiectul de clauze contractuale standard prezentat de AS DK [articolul 28 alineatul (8) din RGPD], CEPD a recomandat includerea textului articolului 28 alineatul (3) litera (a) pentru a asigura securitatea juridică.

[109] Clauzele contractuale standard ale AS slovene în scopul respectării articolului 28 din RGPD, în special clauzele 3.1 și 7.2.

[110] Clauzele contractuale standard ale AS lituaniene în scopul respectării articolului 28 din RGPD, în special clauzele 4.1, 22 și 23.

împuternicită de operator să efectueze prelucrarea datelor cu caracter personal care nu se bazează pe instrucțiunile operatorului și, prin urmare, nu este în numele operatorului, (b) necesitatea ca persoana împuternicită de operator să informeze operatorul[111]; și (c) trimiterea la o astfel de cerință juridică care decurge din legislația UE sau a statelor membre.

104. În acest context, CEPD reamintește că, ca principiu general, contractele nu pot prevala asupra legii. Asta înseamnă că, indiferent dacă clauza prevăzută la articolul 28 alineatul (3) litera (a) din RGPD („*cu excepția cazului în care persoanei împuternicite de operator îi revine această obligație în temeiul dreptului Uniunii sau al dreptului intern care i se aplică*") este inclusă într-un contract, aceasta nu poate împiedica aplicarea de cerințe juridice în plus față de cerințele contractuale sau, în unele cazuri, în conflict cu ele. În plus, în conformitate cu principiul general conform căruia un contract nu creează obligații față de terți, un contract nu poate fi obligatoriu, de exemplu, pentru autoritățile publice ale unui stat membru sau ale unei țări terțe[112].

105. Toate contractele dintre un operator și o persoană împuternicită de operator trebuie să abordeze situațiile în care persoana împuternicită de operator poate fi obligată prin legislație să prelucreze date cu caracter personal altfel decât pe baza instrucțiunilor operatorului. În plus, și obligația persoanei împuternicite de operator de a informa operatorul înainte de a efectua o prelucrare care nu se bazează pe instrucțiunile sale este un element de bază al contractului, care trebuie, de asemenea, inclus [113].

106. Pentru datele cu caracter personal prelucrate în afara SEE, trimiterea la legislația UE sau a statelor membre ar putea să nu fie foarte semnificativă, având în vedere că o persoană împuternicită de un operator din afara SEE se va supune doar în mod excepțional cerințelor legale ale UE sau ale statelor membre. În această privință, CEPD constată că CCS-urile CE pentru transferul internațional, care sunt destinate să îndeplinească, pe lângă cerințele de la articolul 46 alineatul (1) și articolul 46 alineatul (2) litera (d) din RGPD, cerințele de la articolul 28 alineatele (3) și (4) din RGPD[114], nu conțin o formulare similară cu clauza „cu excepția cazului în care" de la articolul 28 alineatul (3) litera (a) din RGPD. Cu toate acestea, cerința de a prelucra date cu caracter personal numai pe baza unor instrucțiuni documentate din partea operatorului, cu excepția cazului în care această obligație este impusă de legislația UE sau a statului membru, este deja abordată indirect prin clauza 8.1 din CCS-urile CE pentru

[111] Articolul 28 alineatul (3) litera (a) din RGPD prevede că, în cazul în care legislația Uniunii sau a unui stat membru impune persoanei împuternicite de operator să prelucreze date cu caracter personal, în acest caz, *„persoana împuternicită de operator notifică această obligație juridică operatorului înainte de prelucrare, cu excepția cazului în care legislația respectivă interzice această informare din motive importante legate de interesul public*;".

[112] De aceea, CCS-urile CE pentru transferul internațional cuprind mai multe garanții care impun exportatorului și importatorului să evalueze cerințele obligatorii ale legislației unei țări terțe înainte de transferul datelor, pentru a se asigura că acestea nu depășesc ce este necesar într-o societate democratică [clauza 14 literele (a)-(d)], impun importatorului să notifice exportatorul în caz de modificări, iar acesta din urmă să acționeze în consecință [clauza 14 literele (e) și (f)] și impun importatorului obligații în caz de acces din partea autorităților publice (clauza 15). Vezi hotărârea CJUE Schrems II, punctele 125 și 141.

[113] În Avizul nr. 18/2021 al CEPD privind proiectul de clauze contractuale standard înaintat de AS lituaniană [articolul 28 alineatul (8) din RGPD], CEPD a recomandat includerea ultimului element al articolului 28 alineatul (3) litera (a) în CCS-uri (și anume obligația persoanei împuternicite de operator de a informa operatorul cu privire la cerința juridică aplicabilă), Avizul CEPD nr. 18/2021, punctul 19.

[114] Vezi considerentul 9 din CCS-urile CE pentru transferul internațional „*În cazul în care prelucrarea implică transferuri de date de la operatori care fac obiectul Regulamentului (UE) 2016/679 către persoane împuternicite de operatori care nu intră sub incidența domeniului de aplicare teritorială a regulamentului menționat sau de la persoane împuternicite de operatori care fac obiectul Regulamentului (UE) 2016/679 către subcontractanți care nu intră sub incidența domeniului de aplicare teritorială a regulamentului menționat, ar trebui, de asemenea, ca clauzele contractuale standard prevăzute în anexa la prezenta decizie să permită îndeplinirea cerințelor prevăzute la articolul 28 alineatele (3) și (4) din Regulamentul (UE) 2016/679*."

transferul internațional [115]. În plus, acest lucru nu înseamnă că obligația de informare prevăzută la articolul 28 alineatul (3) litera (a) din RGPD nu este abordată, având în vedere că CCS-urile CE privind transferul internațional includ în mod explicit necesitatea ca importatorul de date să informeze exportatorul de date dacă nu poate urma instrucțiunile operatorului [116]. În consecință, angajamentul persoanei împuternicite de operator de a informa operatorul în cazul în care se aplică o cerință legală de prelucrare (care decurge din legislația UE sau a statului membru sau din legislația țării terțe) rezultă din CCS-urile CE pentru transferul internațional fără să se folosească formularea exactă „*cu excepția cazului în care persoanei împuternicite de operator îi revine această obligație în temeiul dreptului Uniunii sau al dreptului intern care i se aplică*" de la articolul 28 alineatul (3) litera (a) din RGPD [elementul (c) menționat mai sus].

107. Acest lucru este în conformitate cu obiectivul articolului 28 alineatul (3) litera (a) din RGPD de a se asigura că operatorul este informat atunci când persoana împuternicită de operator este obligată prin lege să prelucreze date cu caracter personal altfel decât la instrucțiunile operatorului.

108. În lumina analizei de mai sus, CEPD consideră că includerea, într-un contract încheiat între operator și persoana împuternicită de operator[117], a excepției prevăzute la articolul 28 alineatul (3) litera (a) din RGPD „*cu excepția cazului în care persoanei împuternicite de operator îi revine această obligație în temeiul dreptului Uniunii sau al dreptului intern care i se aplică*" (textual sau în termeni foarte similari) este foarte recomandată, dar nu strict necesară pentru a fi în conformitate cu articolul alineatul (3) litera (a) din RGPD. Această poziție nu aduce atingere necesității unei obligații contractuale de a

[115] Clauza 8 privind garanțiile de protecție a datelor (Modulul doi: Transferuri de la operator la persoana împuternicită de operator) precizează în secțiunea 8.1 – instrucțiuni:
„(a) Importatorul de date prelucrează datele cu caracter personal numai pe baza unor instrucțiuni documentate din partea exportatorului de date. Exportatorul de date poate da astfel de instrucțiuni pe toată durata contractului.
(b) Importatorul de date îl informează imediat pe exportatorul de date dacă nu este în măsură să urmeze aceste instrucțiuni."
În mod similar, în modulul 3 (Transferuri de la persoana împuternicită de operator la persoana împuternicită de operator), clauza 8 privind garanțiile de protecție a datelor prevede în secțiunea 8.1 - instrucțiuni:
„(a) Exportatorul de date l-a informat pe importatorul de date că acționează în calitate de persoană împuternicită de operator în conformitate cu instrucțiunile operatorului (operatorilor) său (săi), pe care exportatorul de date le pune la dispoziția importatorului de date înainte de prelucrare.
(b) Importatorul de date prelucrează datele cu caracter personal numai pe baza unor instrucțiuni documentate din partea operatorului, astfel cum au fost comunicate importatorului de date de către exportatorul de date, precum și pe baza oricăror instrucțiuni suplimentare documentate din partea exportatorului de date. Aceste instrucțiuni suplimentare nu contravin instrucțiunilor din partea operatorului. Operatorul sau exportatorul de date poate da instrucțiuni documentate suplimentare cu privire la prelucrarea datelor pe întreaga durată a contractului.
(c) Importatorul de date îl informează imediat pe exportatorul de date dacă nu este în măsură să urmeze aceste instrucțiuni. În cazul în care importatorul de date nu este în măsură să urmeze instrucțiunile operatorului, exportatorul de date notifică imediat acest fapt operatorului."

[116] Pe lângă clauza 8.1 (vezi nota de subsol anterioară), clauza 14 prevede în secțiunea 14.e că: „*Importatorul de date este de acord să transmită cu promptitudine o notificare exportatorului de date dacă, după ce a acceptat prezentele clauze și pe durata contractului, are motive să creadă că este sau a intrat sub incidența unei legislații sau a unor practici care nu sunt conforme cu dispozițiile prevăzute la litera (a), inclusiv în urma unei modificări a legislației țării terțe sau a unei măsuri (cum ar fi o cerere de divulgare) care indică o aplicare în practică a acestei legislații care nu este conformă cu dispozițiile prevăzute la litera (a)). [Pentru modulul 3: Exportatorul de date transmite notificarea operatorului.]*"

[117] În special, în cazul în care operatorul și persoana împuternicită de operator se bazează pe propriul lor contract de prelucrare, și nu pe CCS-urile CE operator-persoană împuternicită de operator, pe CCS-urile adoptate de AS în scopul respectării articolului 28 din RGPD sau a CCS-urilor CE pentru transferul internațional. Vezi și considerentul 109 și articolul 28 alineatul (6) din Regulamentul (UE) 2016/679.

informa operatorul atunci când persoana împuternicită de operator este obligată prin lege să prelucreze date cu caracter personal altfel decât la instrucțiunile operatorului, așa cum prevede articolul 28 alineatul (3) litera (a) din RGPD. Când este clar că cerințele juridice ale UE sau ale statelor membre sunt relevante pentru prelucrare, utilizarea formulării de la articolul 28 alineatul (3) litera (a) din RGPD ar contribui la demonstrarea conformității.

109. Acum, CEPD decide dacă un contract care include o excepție mai largă care acoperă și legislația țărilor terțe, cum ar fi, de exemplu, o excepție de la angajamentul de a prelucra datele cu caracter personal numai pe baza unor instrucțiuni documentate din partea operatorului *„cu excepția cazului în care această obligație îi revine în temeiul legii sau a unei ordonanțe obligatorii a unui organism guvernamental*”, reprezintă în sine o încălcare a articolului 28 alineatul (3) litera (a) din RGPD.

110. Această formulare, dacă nu este însoțită de specificații suplimentare, poate cuprinde două situații distincte care trebuie analizate separat în lumina contextului juridic:

- cerința legală sau ordonanța obligatorie avută în vedere decurge din dreptul Uniunii sau din dreptul statelor membre (SEE).
- cerința legală sau ordonanța obligatorie preconizat rezultă din alte legi decât legislația Uniunii sau a statului membru (SEE).

111. Prima situație se încadrează în dispozițiile exprese ale articolului 28 alineatul (3) litera (a) din RGPD, care prevăd un angajament contractual al persoanei împuternicite de operator de a prelucra numai în baza instrucțiunilor documentate ale operatorului *„cu excepția cazului în care persoanei împuternicite de operator îi revine această obligație în temeiul dreptului Uniunii sau al dreptului intern care i se aplică”.* Acest lucru este valabil indiferent dacă prelucrarea datelor cu caracter personal are loc în interiorul sau în afara SEE.

112. Legislația UE, inclusiv RGPD și cerințele juridice ale statelor membre fac parte din aceeași tradiție constituțională ca RGPD, care consacră protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal ca drept fundamental, în temeiul articolului 16 alineatul (1) din Tratatul privind funcționarea Uniunii Europene (denumit în continuare „**TFUE**”) și al articolului 8 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „**carta**”)[118].

113. În cazul în care părțile pot demonstra, pe baza altor elemente ale contractului (contractelor) lor, că numai această primă situație este cuprinsă în formularea *„cu excepția cazului în care această obligație îi revine în temeiul legii sau al unei ordonanțe obligatorii a unui organism guvernamental”*, atunci această formulare nu are impact asupra garanțiilor prevăzute la articolul 28 alineatul (3) litera (a) din RGPD.

114. Vor exista cazuri în care contractul (contractele) părților depășește această primă situație, ceea ce înseamnă că o trimitere la *„lege sau ordonanța obligatorie a unui organism guvernamental*” cuprinde cerințele legale/ordonanțele obligatorii care decurg din alte legi decât dreptul Uniunii sau al statului membru (SEE) (a doua situație).

115. CEPD observă că cerințele de prelucrare a datelor bazate pe alte legi decât legislația Uniunii sau a statelor membre (SEE) nu împărtășesc tradiția constituțională în sine și nu pot fi considerate automat în același mod ca cele din ordinea juridică a UE (în lumina articolului 44 din RGPD). În acest sens, CEPD reamintește că, în temeiul articolului 6 din RGPD, termenii „obligație legală”, „interes public” și „autoritate publică” se referă la dreptul Uniunii sau al statelor membre[119]. De asemenea, CEPD observă că articolul 29 din RGPD privind prelucrarea sub autoritatea operatorului sau a persoanei împuternicite de operator prevede că *„[p]ersoana împuternicită de operator și orice persoană care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator, care are acces la date cu caracter personal, nu le prelucrează decât la cererea operatorului, cu excepția cazului în care dreptul Uniunii sau dreptul unui stat membru îl obligă să facă acest lucru.*” (evidențiere adăugată)

[118] Considerentul 1 din RGPD face trimitere la articolul 16 alineatul (1) din Tratatul privind funcționarea Uniunii Europene („TFUE”) și la articolul 8 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene („carta”). Articolul 52 alineatul (1) din cartă precizează că *„Orice restrângere a exercițiului drepturilor și libertăților recunoscute prin prezenta cartă trebuie să fie prevăzută de lege și să respecte substanța acestor drepturi și libertăți. Prin respectarea principiului proporționalității, pot fi impuse restrângeri numai în cazul în care acestea sunt necesare și numai dacă răspund efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți*”.

[119] Articolul 6 alineatul (3) din RGPD prevede că, în cazul în care temeiul juridic al prelucrării este „obligația legală” [articolul 6 alineatul (1) litera (c) din RGPD] sau „o sarcină care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul” [articolul 6 alineatul (1) litera (e) din RGPD], aceasta se referă la dispozițiile prevăzute în dreptul Uniunii sau în dreptul intern care se aplică operatorului. În ceea ce privește articolul 6 din RGPD, considerentul 40 din RGPD explică faptul că, în cazul în care temeiul juridic pentru prelucrare este stabilit prin lege, aceasta înseamnă *„fie în prezentul regulament, fie în alte acte legislative ale Uniunii sau ale statelor membre menționate în prezentul regulament*”. Articolul 49 alineatul (4) din RGPD prevede că numai interesele publice recunoscute în dreptul Uniunii sau în dreptul statului membru căruia îi este supus operatorul pot duce la aplicarea acestei derogări.

116. În contextul transferurilor, este previzibil că cerințele legale pot decurge și din alte acte legislative decât dreptul Uniunii sau cel al statelor membre. În cazul în care au loc transferuri, CEPD reamintește că capitolul V din RGPD se aplică în plus față de articolul 28 din RGPD. CEPD consideră că, în ceea ce privește datele cu caracter personal prelucrate în afara SEE, articolul 28 alineatul (3) litera (a) din RGPD nu împiedică - în principiu - includerea, în contract, a unor dispoziții care abordează cerințele legislației țărilor terțe privind prelucrarea datelor cu caracter personal transferate. Asemenea dispoziții pot fi incluse în special pentru a asigura conformitatea cu capitolul V din RGPD, însă este foarte puțin probabil ca simpla includere a cuvintelor *„cu excepția cazului în care această obligație îi revine în temeiul legii sau al unei ordonanțe obligatorii a unui organism guvernamental”* să fie suficientă.

117. În acest context, CEPD observă că CCS-urile Comisiei Europene pentru transferul internațional abordează în mod specific „Legislația locală și practicile locale care afectează respectarea clauzelor” din clauza 14 și „Obligațiile importatorului de date în cazul accesului autorităților publice” din clauza 15. Înainte de semnarea CCS-urilor, părțile trebuie să evalueze dacă există legi și practici locale care afectează respectarea clauzelor (clauza 14 din CCS-urile CE pentru transferul internațional). Clauza 14 solicită părților să garanteze că nu au cunoștință de legile și practicile din țara terță în care își are sediul importatorul care l-ar împiedica să-și îndeplinească obligațiile care îi revin în temeiul CCS-urilor CE pentru transferul internațional, în urma unei evaluări, de către importator, a acestor legi și practici, și solicită importatorului să notifice imediat exportatorului orice schimbare, caz în care fie exportatorul identifică măsurile adecvate pentru a rezolva situația, fie clauza 14 îi permite să suspende transferul și chiar să rezilieze contractul. Clauza 15 impune anumite obligații importatorului de date în cazul accesului de către autoritățile publice din țări terțe. Stabilește o serie de etape pe care importatorul de date trebuie să le parcurgă în cazul în care se confruntă cu accesul administrației publice din țări terțe (fie la cerere, fie direct), pentru a se asigura (în cele din urmă) că operatorul este informat. Pe lângă obligația de a notifica exportatorul de date, importatorul are, printre altele, obligația de a examina legalitatea cererii de acces și de a documenta această evaluare juridică, precum și obligația de a contesta cererea în anumite cazuri. Ulterior, exportatorul de date - în consultare cu operatorul, când exportatorul de date nu este operatorul - va fi în măsură să ia măsurile necesare, inclusiv posibila suspendare a transferului sau încetarea CCS-urilor CE pentru transferul internațional. Conformitatea oricăror transferuri (ulterioare) către guvernul țării terțe cu RGPD va depinde de analiza de la caz la caz (printre altele, în ceea ce privește temeiul legal, controlul și respectarea capitolului V din RGPD). În conformitate cu modulul 3 din CCS-urile CE pentru transferul internațional (persoană împuternicită de operator-persoană împuternicită de operator), importatorul/persoana împuternicită de operator are obligația de a pune evaluarea juridică la dispoziția exportatorului. În acest sens, CEPD trimite și la punctele 88-89 și 106 de mai sus.

118. În plus, conform CCS-urilor CE pentru transferul internațional, atât exportatorul, cât și importatorul sunt obligați să se asigure că legislația țării terțe de destinație permite importatorului să respecte CCS-urile pentru transferul internațional înainte de a transfera date cu caracter personal către țara terță respectivă[120]. În cazul în care persoana împuternicită de operator exportă date cu caracter personal în numele operatorului, această obligație revine și operatorului (vezi și punctul 79 și următoarele de mai sus).

119. În mod similar, recomandările RCO-operator și criteriile de referință RCO-persoană împuternicită de operator stabilesc și un set de obligații în cazul în care un membru al RCO se confruntă cu un conflict

[120] Hotărârea CJUE *Schrems II*, punctul 141. Vezi și CCS-urile CE pentru transferul internațional, clauza 14 literele (a)-(d).

între legislația sa locală și RCO[121] și/sau primește o cerere de divulgare din partea unei autorități de aplicare a legii sau a unui organism de securitate a statului[122]. Mai precis, Recomandările CEPD nr. 1/2022[123] arată că Regulile corporatiste obligatorii pentru operatori (RCO-O) trebuie să conțină clauze care să abordeze legile și practicile locale care afectează conformitatea cu RCO-O (secțiunea 5.4.1), precum și obligațiile importatorului de date în cazul cererilor de acces din partea guvernului (secțiunea 5.4.2). RCO-O pot servi drept mecanism de transfer pentru transferurile către persoanele împuternicite de operator din cadrul grupului.

120. În cazurile în care transferurile fac obiectul unor decizii privind caracterul adecvat al nivelului de protecție, legislația privind „*accesul autorităților publice la datele cu caracter personal, precum și punerea în aplicare a acestei legislații*" este unul dintre elementele pe care Comisia Europeană trebuie să le ia în considerare când evaluează caracterul adecvat al nivelului de protecție, în temeiul articolului 45 alineatul (2) litera (a) din RGPD[124].

121. Ceea ce au în comun deciziile privind caracterul adecvat [125], CCS-urile CE pentru transferul internațional [126] și recomandările și criteriile de referință RCO [127] este înțelegerea faptului că legile și practicile unei țări terțe care respectă esența drepturilor și libertăților fundamentale consacrate în TFUE, în cartă și în

[121] Secțiunea 5.4.1 „Legislația locală și practicile locale care afectează respectarea RCO-O", Recomandarea nr. 1/2022 a CEPD privind cererea de aprobare și privind elementele și principiile care trebuie menționate în regulile corporatiste obligatorii pentru operatori (articolul 47 din RGPD). Secțiunea 6.3 „Necesitatea de transparență în cazul în care legislația națională împiedică grupul să respecte regulile corporatiste obligatorii" din documentul de lucru al Grupului de lucru „articolul 29" care stabilește un tabel cu elementele și principiile care se regăsesc în regulile corporatiste obligatorii pentru persoanele împuternicite de operator, WP257 rev.01, aprobat de CEPD la 25 mai 2018.

[122] Secțiunea 5.4.2 „Obligațiile importatorului de date în cazul cererilor de acces din partea guvernului", Recomandările CEPD nr. 1/2022 privind cererea de aprobare și elementele și principiile care se regăsesc în regulile corporatiste obligatorii (articolul 47 din RGPD); vezi și secțiunea 6.3 „Necesitatea de a fi transparent în cazul în care legislația națională împiedică grupul să respecte RCO-urile", documentul de lucru care stabilește un tabel cu elementele și principiile care se regăsesc în regulile corporatiste obligatorii pentru operatori, WP257 rev.01.

[123] Recomandările CEPD nr. 1/2022 privind cererea de aprobare și elementele și principiile care trebuie să se regăsească în regulile corporatiste obligatorii pentru operatori (articolul 47 din RGPD)

[124] CJUE a abordat acest element în hotărârile sale Schrems I și Schrems II. Hotărârea CJUE din 6 octombrie 2015, *Maximillian Schrems/Comisarul pentru protecția datelor*, (denumită în continuare „hotărârea CJUE Schrems I"), cauza C-362/14, ECLI:EU:C:2015:650, punctul 91 și următoarele. Hotărârea CJUE Schrems II, punctele 141, 174-177, 187-189.

[125] Vezi articolul 45 alineatul (2) litera (a) din RGPD care prevede că Comisia Europeană va ține seama de „*statul de drept, respectarea drepturilor omului și a libertăților fundamentale, legislația relevantă, atât generală, cât și sectorială, inclusiv privind securitatea publică, apărarea, securitatea națională și dreptul penal, precum și accesul autorităților publice la datele cu caracter personal, precum și punerea în aplicare a acestei legislații, normele de protecție a datelor, normele profesionale și măsurile de securitate, inclusiv normele privind transferul ulterior de date cu caracter personal către o altă țară terță sau organizație internațională, care sunt respectate în țara terță respectivă sau în organizația internațională respectivă, jurisprudența, precum și existența unor drepturi efective și opozabile ale persoanelor vizate și a unor reparații efective pe cale administrativă și judiciară pentru persoanele vizate ale căror date cu caracter personal sunt transferate*;". Vezi și Criteriile de referință privind caracterul adecvat al nivelului de protecție, adoptate de Grupul de lucru „Articolul 29" (WP254 rev.01), adoptate la 6 februarie 2018 și avizate de CEPD la 25 mai 2018. Conceptul de „nivel adecvat de protecție" a fost dezvoltat în continuare de CJUE în hotărârile Schrems I (punctele 73 și 74) și Schrems II (punctul 94).

[126] Clauza 14 litera (a) din Clauzele contractuale tip ale Comisiei Europene privind transferul internațional de date.

[127] Acest lucru este explicit în Recomandările CEPD nr. 1/2022 (recomandările RCO-O), versiunea 2.1, la punctele 5.4.1 și 5.4.2. Aceeași înțelegere stă implicit la baza secțiunii 6.3 „Necesitatea de a fi transparentă în cazul în care legislația națională împiedică grupul să respecte RCO-urile" din documentul de lucru al Grupului de lucru „Articolul 29", care stabilește un tabel cu elementele și principiile care se regăsesc în regulile corporatiste obligatorii pentru persoanele împuternicite de operator, WP 257 rev.01, aprobat de CEPD la 25 mai 2018.

RGPD și care nu depășesc ceea ce este necesar și proporțional într-o societate democratică pentru a proteja unul dintre obiectivele enumerate la articolul 23 alineatul (1) din RGPD, nu vor submina nivelul de protecție asigurat de RGPD[128]. Din acest motiv, CCS-urile CE pentru transferuri internaționale[129] și recomandările și referințele RCO[130] conțin dispoziții care acordă diferite consecințe legilor și practicilor, în funcție de măsura în care subminează nivelul de protecție asigurat de RGPD. Contractele ad-hoc bazate pe articolul 46 alineatul (3) litera (a) din RGPD ar trebui să conțină, de asemenea, dispoziții similare.[131]

122. Din cele de mai sus reiese clar că, atunci când legislația țării terțe impune persoanei împuternicite de operator să prelucreze date cu caracter personal altfel decât pe baza instrucțiunilor operatorului, nivelul de protecție prevăzut de RGPD va fi respectat numai dacă legile menționate îndeplinesc condițiile menționate mai sus. În orice caz, persoana împuternicită de operator trebuie să pună în aplicare măsuri suplimentare în cazul în care condițiile menționate anterior nu sunt îndeplinite, iar contractul trebuie să asigure îndeplinirea acestor condiții.

123. Atunci când persoana împuternicită de operator prelucrează date cu caracter personal în cadrul SEE, aceasta se poate confrunta în continuare cu legislația țărilor terțe, în anumite circumstanțe. CEPD subliniază că adăugarea în contract a unei trimiteri la legislația țării terțe nu exonerează persoana împuternicită de operator de obligațiile care îi revin în temeiul RGPD.

124. În lumina analizei de mai sus, CEPD consideră că includerea unei formulări similare cu „*cu excepția cazului în care această obligație îi revine în temeiul legii sau al unei ordonanțe obligatorii a unui organism guvernamental*" este o prerogativă a libertății contractuale a părților și nu încalcă articolul 28 alineatul (3) litera (a) din RGPD per se. Acest lucru nu aduce atingere obligației de a respecta RGPD ori de câte ori sunt prelucrate date cu caracter personal. În plus, o asemenea clauză nu exonerează operatorul și persoana împuternicită de operator de respectarea obligațiilor care le revin în temeiul RGPD, în special în ceea ce privește informațiile care trebuie furnizate operatorului și - după caz - condițiile pentru transferurile internaționale de date cu caracter personal prelucrate în numele operatorului.[132]

125. În sfârșit, cererea solicită o întrebare de monitorizare:

> Dacă răspunsul la întrebarea 2a este negativ, o asemenea excepție extinsă trebuie interpretată ca instrucțiune documentată a operatorului în sensul articolului 28 alineatul (3) litera (a) din RGPD?

126. În lumina răspunsului de mai sus, CEPD consideră că întrebarea rămasă este dacă părțile pot pretinde că formularea „*cu excepția cazului în care această obligație îi revine în temeiul legii sau al unei ordonanțe obligatorii a unui organism guvernamental*" (textual sau în termeni foarte similari) din contractul lor trebuie interpretată ca o instrucțiune documentată a operatorului în sensul articolului 28 alineatul (3) litera (a) din RGPD.

---

[128] Recomandările CEPD nr. 1/2020 privind măsurile care completează instrumentele de transfer pentru a asigura conformitatea cu nivelul UE de protecție a datelor cu caracter personal, v. 2.0, punctul 38, și Recomandările CEPD nr. 2/2020 privind garanțiile esențiale europene pentru măsurile de supraveghere, punctele 22 și 24.

[129] Clauza 14 din CCS-urile CE pentru transferul internațional de date.

[130] Vezi nota de subsol 127.

[131] Vezi Recomandările nr. 1/2020 privind măsurile care completează instrumentele de transfer pentru a asigura conformitatea cu nivelul UE de protecție a datelor cu caracter personal, v. 2.0, punctul 66

[132] În special, obligația operatorului de a se asigura că, în ceea ce privește prelucrarea în afara SEE, numai legislația țării terțe care asigură un nivel de protecție esențial echivalent poate impune prelucrarea de către persoana împuternicită de operator. Vezi și punctele 116 - 122 de mai sus.

127. CEPD consideră, în primul rând, că acest argument poate fi acceptat în cazul în care cerința legală sau ordonanța obligatorie decurge din dreptul Uniunii sau al statului membru (SEE).

128. CEPD observă că noțiunea de „instrucțiuni", așa cum este utilizată la articolul 28 alineatul (3) litera (a) din RGPD, se referă în mod specific la operatorul care stabilește ce prelucrare de date se preconizează că va efectua persoana împuternicită de operator în numele său și în ce mod.[133] Orice dispoziție pe care operatorul o include în contractul cu furnizorul său de servicii / persoana împuternicită de operator, care nu constă într-o cerere de a efectua prelucrarea datelor cu caracter personal în numele operatorului, de asemenea, nu se califică drept instrucțiune în sensul articolului 28 alineatul (3) litera (a) din RGPD. În plus, instrucțiunile operatorului trebuie să fie suficient de precise pentru a acoperi o prelucrare specifică a datelor cu caracter personal, ceea ce nu este cazul cu formularea în cauză. În plus, operatorul ar fi întotdeauna în măsură (ar trebui să fie) - și obligat din punct de vedere juridic în măsura în care o instrucțiune de prelucrare a datelor cu caracter personal în numele operatorului ar încălca RGPD - să retragă o astfel de instrucțiune. Persoana împuternicită de operator ar trebui apoi să se conformeze retragerii instrucțiunii operatorului și să oprească prelucrarea.

129. Dând instrucțiuni persoanei împuternicite de operator, operatorul pune în practică stabilirea scopurilor și mijloacelor de prelucrare a datelor, în special prin exercitarea unei influențe asupra elementelor-cheie ale prelucrării[134]. În principiu, influența operatorului asupra prelucrării datelor cu caracter personal încetează în cazul în care legislația UE sau a statului membru stabilește cerințe pentru persoana împuternicită de operator de a efectua prelucrări de date cu caracter personal pe care operatorul nu este în măsură să le dirijeze sau să le oprească[135]. Deși operatorul ar putea să reamintească persoanei împuternicite de operator să respecte legislația UE sau a statelor membre, acest lucru nu poate fi înțeles ca o instrucțiune în sensul articolului 28 alineatul (3) litera (a) din RGPD[136]. RGPD însuși recunoaște această stare de fapt, tocmai prin faptul că persoana împuternicită de operator trebuie să prelucreze numai la instrucțiunile documentate ale operatorului, cu excepția cazului în care legislația Uniunii sau a statului membru la care este supusă persoana împuternicită de operator îi impune acest lucru [articolul 28 alineatul (3) litera (a) din RGPD] și trebuie să informeze imediat operatorul dacă o instrucțiune încalcă RGPD [articolul 28 alineatul (3) din RGPD ultimul paragraf].

130. CEPD consideră că raționamentul de mai sus se aplică și în cazul în care cerința legală sau ordonanța obligatorie rezultă din legislația unei țări terțe. În această situație, legea în cauză limitează influența pe care operatorul o poate exercita asupra prelucrării datelor.

131. În plus față de cele de mai sus, o clauză prin care o persoană împuternicită de operator se angajează să prelucreze date cu caracter personal numai pe baza unor instrucțiuni documentate din partea operatorului *„cu excepția cazului în care această obligație îi revine în temeiul legii sau al unei ordonanțe obligatorii a unui organism guvernamental"* indică în sine că prelucrarea în baza instrucțiunilor operatorului este regula, iar excepția există tocmai pentru prelucrarea nu la instrucțiunile operatorului

[133] Orientările CEPD nr. 7/2020, punctul 116.

[134] Orientările CEPD nr. 7/2020, punctul 20.

[135] În acest sens, situația ar putea fi atunci cea prevăzută de articolul 4 alineatul (7) din RGPD, care prevede că, în cazul în care scopurile și mijloacele de prelucrare sunt stabilite prin dreptul Uniunii sau al statului membru, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute de dreptul Uniunii sau al statului membru. Vezi hotărârea CJUE din 11 ianuarie 2024, *Belgian State (Données traitées par un journal officiel),* cauza C-231/22, ECLI:EU:C:2024:7, punctele 28-30, 35 și 39; Orientările CEPD nr. 7/2020, punctele 22-24.

[136] Mai degrabă, un astfel de memento va fi considerat ca fiind punerea în aplicare de către operator a unor garanții contractuale pentru a se asigura că prelucrarea în numele operatorului va respecta toate cerințele RGPD și va asigura protecția drepturilor persoanei vizate.

(după cum se arată prin cuvintele „cu excepția cazului"). În plus, rămâne la latitudinea persoanei împuternicite de operator dacă se conformează obligației legale sau ordonanței obligatorii la care este supusă sau dacă se confruntă cu consecințele juridice ale nerespectării .

132. Pe această bază, CEPD concluzionează că *„cu excepția cazului în care această obligație îi revine în temeiul legii sau al unei ordonanțe obligatorii a unui organism guvernamental*" (exact sau în termeni foarte similari) nu poate fi interpretat ca instrucțiune documentată a operatorului. Operatorul rămâne responsabil în cazul în care nu s-a asigurat că persoana împuternicită de operator (subcontractantul) prelucrează datele cu caracter personal numai conform instrucțiunilor sale documentate. Acest lucru nu se aplică însă dacă prelucrarea este impusă de legislația UE sau a unui stat membru sau, în cazul prelucrării în afara SEE, este impusă de legislația unei țări terțe căreia i se supune persoana împuternicită de operator (subcontractantul), iar legislația respectivă asigură un nivel de protecție esențial echivalent.

Pentru Comitetul European pentru Protecția Datelor

Președinte

(Anu Talus)