Recomandările 01/2021 cu privire la criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul Directivei privind protecția datelor în materie de asigurare a respectării legii

Adoptate la 2 februarie 2021

Istoric versiuni

Versiunea 1.1	6 iulie 2021	Schimbări legate de formatare
Versiunea 1.0	2 februarie 2021	Adoptarea recomandărilor

Cuprins

Comitetul european pentru protecția datelor (CEPD),

având în vedere articolul 51 alineatul (1) litera (b) din Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului[1],

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

ADOPTĂ URMĂTOARELE RECOMANDĂRI:

1. INTRODUCERE

1. Grupul de lucru „Articolul 29" (WP29) a publicat un document de lucru[2] referitor la criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul Regulamentului general privind protecția datelor (RGPD)[3]. Acest document de lucru a fost aprobat de Comitetul european pentru protecția datelor (CEPD) în cadrul primei sale sesiuni plenare.

2. Astfel cum se menționează în Declarația nr. 21 anexată la Tratatul de la Lisabona, s-ar putea dovedi necesare norme specifice privind protecția datelor cu caracter personal și libera circulație a acestor date în domeniul cooperării judiciare în materie penală și al cooperării polițienești în temeiul articolului 16 din Tratatul privind funcționarea Uniunii Europene (TFUE), având în vedere natura specifică a acestor domenii.

3. Pe această bază, legiuitorul UE a adoptat Directiva (UE) 2016/680 (Directiva privind protecția datelor în materie de asigurare a respectării legii, denumită în continuare „LED") de stabilire a unor norme specifice privind prelucrarea datelor cu caracter personal de către autoritățile competente în scopul **prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora**.

4. LED stabilește motivele care permit transferul de date cu caracter personal către o țară terță sau către o organizație internațională în acest context. Unul dintre motivele unui astfel de transfer este decizia Comisiei Europene potrivit căreia țara terță sau organizația internațională în cauză asigură un nivel adecvat de protecție.

[1] JO L 119, 4.5.2016, p. 89.
[2] WP254.rev01 adoptat de WP29 la 28 noiembrie 2017, astfel cum a fost revizuit ultima dată și adoptat la 6 februarie 2018. Acesta actualizează capitolul I din documentul de lucru „Transferurile de date cu caracter personal către țările terțe: aplicarea articolelor 25 și 26 din Directiva UE privind protecția datelor", WP12, adoptat de WP29 la 24 iulie 1998.
[3] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 26 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), JO L 119, 4.5.2016, p. 1.

5. Dacă documentul de lucru WP254.rev01 referitor la criteriile de referință privind caracterul adecvat al nivelului de protecție urmărește să ofere orientări Comisiei Europene cu privire la nivelul de protecție a datelor în țările terțe și în organizațiile internaționale în temeiul RGPD, prezentul document urmărește să ofere orientări similare în temeiul LED. În acest context, sunt stabilite principiile fundamentale de protecție a datelor care trebuie să fie prezente în cadrul juridic al unei țări terțe sau al unei organizații internaționale pentru a asigura echivalența esențială cu cadrul UE în domeniul de aplicare al LED (și anume, pentru prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor). În plus, documentul ar putea ghida țările terțe și organizațiile internaționale interesate să obțină un caracter adecvat al nivelului de protecție.

6. Prezentul document se axează exclusiv pe deciziile privind caracterul adecvat al nivelului de protecție. Acestea sunt acte de punere în aplicare ale Comisiei Europene în conformitate cu articolul 36 alineatul (3) din LED.

2. CONCEPTUL DE CARACTER ADECVAT AL NIVELULUI DE PROTECȚIE

7. LED stabilește normele pentru transferul datelor cu caracter personal către țări terțe și organizații internaționale, în măsura în care astfel de transferuri intră în domeniul său de aplicare. Normele privind transferurile internaționale de date cu caracter personal sunt prevăzute în capitolul V din LED, în special la articolele 35-39.

8. În temeiul articolului 36 din LED, transferurile de date către o țară terță sau o organizație internațională pot avea loc dacă țara terță, un teritoriu sau unul sau mai multe sectoare specificate din aceasta sau organizația internațională respectivă asigură un nivel adecvat de protecție. Din jurisprudența Curții de Justiție a Uniunii Europene (CJUE)[4] reiese că această dispoziție trebuie interpretată în lumina articolul 35 din LED, intitulat „Principii generale pentru transferurile de date cu caracter personal", care prevede că „toate dispozițiile [din capitolul V din LED] se aplică pentru a se asigura că nivelul de protecție a persoanelor fizice asigurat prin prezenta directivă nu este subminat".

9. În cazul în care Comisia Europeană a decis că acest nivel adecvat de protecție este asigurat, transferurile de date cu caracter personal către țara terță, teritoriul, sectorul sau organizația internațională în cauză pot avea loc, fără a fi necesară obținerea unei autorizații speciale, cu excepția cazului în care un alt stat membru de la care au fost obținute datele trebuie să își acorde autorizația pentru transfer, astfel cum se prevede la articolele 35 și 36 și în considerentul 66 din LED. Acest lucru nu aduce atingere necesității prelucrării datelor de către autoritățile statelor membre în cauză pentru a se conforma dispozițiilor naționale adoptate în temeiul Directivei (UE) 2016/680.

10. Acest concept de „nivel adecvat de protecție", care exista deja în temeiul Directivei 95/46[5] și al Deciziei-cadru 2008/977/JAI[6] a Consiliului, a fost dezvoltat în continuare de CJUE în acest context și, recent, în cadrul RGPD.

[4] Cauza C-311/18, Data Protection Commissioner/Facebook Ireland Ltd și Maximillian Schrems, 16 iulie 2020, ECLI:EU:C:2020:559, punctul 92 (Schrems II).
[5] Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, JO L 281, 23.11.1995, p. 31.
[6] Decizia-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală, JO L 350, 30.12.2008, p. 60.

11. Astfel cum a precizat CJUE, deși nivelul de protecție din țara terță trebuie să fie în esență echivalent cu cel garantat în UE, „mijloacele la care această țară terță a recurs, în această privință, pentru a asigura un astfel de nivel de protecție pot fi diferite de cele puse în aplicare în cadrul Uniunii", totuși aceste mijloace trebuie „să se dovedească în practică efective"[7]. Prin urmare, standardul de adecvare nu impune reflectarea punctuală a legislației UE, ci stabilirea cerințelor esențiale - de bază ale legislației respective.

12. În acest context, Curtea a clarificat și faptul că o decizie a Comisiei privind caracterul adecvat al nivelului de protecție ar trebui să cuprindă orice constatare în privința existenței în țara terță a unor norme adoptate de această țară destinate să limiteze eventualele ingerințe în drepturile fundamentale ale persoanelor ale căror date sunt transferate din Uniunea Europeană către această țară terță, ingerințe pe care entități de stat din această țară ar fi *autorizate* să le practice atunci când urmăresc scopuri legitime precum securitatea națională[8].

13. Scopul deciziilor privind caracterul adecvat al nivelului de protecție adoptate de Comisia Europeană este de a confirma în mod oficial, cu efecte obligatorii asupra statelor membre[9], inclusiv asupra autorităților competente în materie de protecție a datelor ale acestora[10], că nivelul de protecție a datelor într-o țară terță sau o organizație internațională este, în esență, echivalent cu nivelul de protecție a datelor din Uniunea Europeană. Țara terță ar trebui să ofere garanții care să asigure un nivel adecvat de protecție, echivalent în esență celui asigurat în cadrul Uniunii, în special atunci când datele sunt prelucrate în unul sau mai multe sectoare specifice[11].

14. Caracterul adecvat al nivelului de protecție poate fi obținut prin intermediul unei combinații de drepturi pentru persoanele vizate și obligații pentru cei care prelucrează date sau care exercită control asupra prelucrării, precum și prin supravegherea de către organisme independente. Cu toate acestea, normele de protecție a datelor sunt eficace numai dacă sunt executorii și sunt respectate în practică. Prin urmare, este necesar să se ia în considerare nu doar conținutul normelor aplicabile transferului de date cu caracter personal către o țară terță sau o organizație internațională, ci și sistemul existent pentru asigurarea eficacității acestor norme. Mecanismele eficiente de asigurare a respectării sunt de o importanță fundamentală pentru eficacitatea normelor de protecție a datelor[12].

---

[7] Cauza C−362/14, Maximilian Schrems/Data Protection Commissioner, 6 octombrie 2015, ECLI:EU:C:2015:650, punctele 73 și 74 (Schrems I).
[8] Schrems I, punctul 88.
[9] Articolul 288 din TFUE.
[10] Schrems I, punctul 52.
[11] Considerentul 67 din LED.
[12] Schrems I, punctele 72-74 și Avizul 1/15 al CJUE privind proiectul de acord dintre Canada și Uniunea Europeană, 26 iulie 2017, ECLI:EU:C:2017:592 (Avizul 1/15), punctul 134: „Acest drept la protecția datelor cu caracter personal impune printre altele să se asigure continuitatea nivelului ridicat al protecției libertăților și drepturilor fundamentale conferit de dreptul Uniunii în cazul transferului de date cu caracter personal din Uniune către o țară terță. Chiar dacă mijloacele pentru a garanta un astfel de nivel de protecție pot fi diferite de cele puse în aplicare în cadrul Uniunii pentru a garanta respectarea cerințelor care decurg din dreptul Uniunii, aceste mijloace trebuie totuși să se dovedească în practică efective în scopul de a asigura o protecție în esență echivalentă cu cea garantată în cadrul Uniunii."

3. ASPECTE PROCEDURALE PENTRU CONSTATĂRILE PRIVIND CARACTERUL ADECVAT AL NIVELULUI DE PROTECȚIE ÎN TEMEIUL LED

15. Pentru ca CEPD să își îndeplinească misiunea de consiliere a Comisiei Europene în conformitate cu articolul 51 alineatul (1) litera (g) din LED, acesta ar trebui să primească întreaga documentație relevantă, inclusiv corespondența relevantă și constatările Comisiei Europene. Este absolut necesar ca toate documentele relevante să fie transmise către CEPD cu suficient timp înainte și traduse în limba engleză pentru a permite discuții în cunoștință de cauză și utile înainte de adoptarea finală a deciziilor privind caracterul adecvat al nivelului de protecție. În cazul în care cadrul legislativ este complex, aceasta ar trebui să includă orice raport întocmit cu privire la nivelul de protecție a datelor din țara terță sau organizația internațională respectivă. În orice caz, informațiile furnizate de Comisia Europeană ar trebui să fie exhaustive și să permită CEPD să evalueze analiza efectuată de Comisie cu privire la nivelul de protecție a datelor din țara terță sau organizația internațională respectivă.

16. CEPD va emite un aviz cu privire la constatările Comisiei Europene în timp util, identificând deficiențele cadrului de adecvare, dacă este cazul, și furnizând posibile recomandări acolo unde este necesar.

17. În conformitate cu articolul 36 alineatul (4) din LED, Comisiei Europene îi revine sarcina de a monitoriza - în permanență - evoluțiile care ar putea afecta funcționarea unei decizii privind caracterul adecvat al nivelului de protecție.

18. Articolul 36 alineatul (3) din LED prevede că trebuie să se efectueze o revizuire periodică cel puțin o dată la patru ani. Acesta este, însă, un interval de timp general care trebuie ajustat pentru fiecare țară terță sau organizație internațională printr-o decizie privind caracterul adecvat al nivelului de protecție. În funcție de circumstanțele specifice ale fiecărui caz, ar putea fi justificat un ciclu de revizuire mai scurt. De asemenea, incidentele sau alte informații despre cadrul juridic din țara terță sau organizația internațională în cauză sau despre modificarea acestuia ar putea determina necesitatea unei revizuiri înainte de termen. În plus, pare adecvat ca o primă revizuire a unei decizii complet noi privind caracterul adecvat al nivelului de protecție să fie efectuată destul de curând și ca ciclul de revizuire să fie adaptat progresiv în funcție de rezultat.

19. Având în vedere mandatul de a furniza Comisiei Europene un aviz cu privire la faptul că țara terță, un teritoriu sau unul sau mai multe sectoare specificate din țara terță sau o organizație internațională asigură sau nu mai asigură un nivel adecvat de protecție, CEPD trebuie să primească, în timp util, informații semnificative privind monitorizarea evoluțiilor relevante din respectiva țară terță sau organizație internațională de la Comisia Europeană. Prin urmare, CEPD ar trebui să fie informat cu privire la orice proces și misiune de revizuire în țara terță sau la organizația internațională respectivă. CEPD recomandă să fie invitat să participe la aceste procese și misiuni de revizuire, astfel cum a fost prevăzut în Decizia privind Scutul de confidențialitate și cum este prevăzut în decizia privind caracterul adecvat al nivelului de protecție referitoare la Japonia.

20. De asemenea, ar trebui remarcat faptul că, în conformitate cu articolul 36 alineatul (5) din LED, Comisia Europeană are competența, în cazul în care țara terță sau organizația internațională nu mai asigură un nivel de protecție adecvat, să abroge, să modifice sau să suspende deciziile existente privind caracterul adecvat al nivelului de protecție. Procedura de abrogare, modificare

sau suspendare implică solicitarea avizului CEPD în conformitate cu articolul 51 alineatul (1) litera (g) din LED.

21. În plus, fără a aduce atingere competențelor autorităților de urmărire penală, autoritățile de supraveghere ar trebui să aibă și competența de a aduce în atenția autorităților judiciare cazurile de încălcare a acestei directive sau de a se implica în proceduri judiciare[13]. Reiese, în special din hotărârea Schrems I a CJUE, că autoritățile de protecție a datelor trebuie să se poată implica în proceduri judiciare în fața instanțelor naționale în cazul în care constată că o persoană are o cerere întemeiată împotriva unei decizii privind caracterul adecvat al nivelului de protecție[14]. Hotărârea Schrems II a confirmat această evaluare[15].

4. STANDARDELE UE PRIVIND CARACTERUL ADECVAT AL NIVELULUI DE PROTECȚIE ÎN COOPERAREA POLIȚIENEASCĂ ȘI ÎN COOPERAREA JUDICIARĂ ÎN MATERIE PENALĂ

22. Pe fond, deciziile privind caracterul adecvat al nivelului de protecție ar trebui să se axeze pe evaluarea legislației existente a țării terțe în cauză în ansamblu, teoretic și practic, având în vedere criteriile de evaluare prevăzute la articolul 36 din LED. Sistemul unei țări terțe sau al unei organizații internaționale trebuie să conțină următoarele principii și mecanisme fundamentale de protecție a datelor referitoare la aspectele generale, la procedură și la asigurarea respectării.

23. Articolul 36 alineatul (2) din LED stabilește elementele de care Comisia Europeană trebuie să țină seama atunci când evaluează caracterul adecvat al nivelului de protecție dintr-o țară terță sau o organizație internațională.

24. În special, Comisia ia în considerare statul de drept, respectarea drepturilor omului și a libertăților fundamentale[16], legislația relevantă, precum și punerea în aplicare a acestei legislații, drepturile efective și opozabile ale persoanelor vizate și reparații efective pe cale administrativă și judiciară pentru persoanele vizate ale căror date cu caracter personal sunt transferate, existența și

[13] A se vedea articolul 47 alineatul (5) din LED și considerentul 82.

[14] A se vedea Schrems I, punctul 65: „În această privință, revine legiuitorului național sarcina de a prevedea căi de atac care să permită autorității naționale de supraveghere în cauză să invoce motivele pe care le consideră întemeiate în fața instanțelor naționale, astfel încât acestea din urmă să efectueze, dacă împărtășesc îndoielile acestei autorități în ceea ce privește validitatea deciziei Comisiei, o trimitere preliminară în vederea examinării validității acestei decizii".

[15] A se vedea Schrems II, punctul 120: „Astfel, chiar în prezența unei decizii privind caracterul adecvat al nivelului de protecție a Comisiei, autoritatea națională de supraveghere competentă, sesizată de o persoană cu o plângere privind protecția drepturilor și libertăților sale în ceea ce privește o prelucrare a datelor cu caracter personal care o privesc, trebuie să poată examina în condiții de independență deplină dacă transferul acestor date respectă cerințele stabilite de RGPD și, dacă este cazul, să introducă o cale de atac în fața instanțelor naționale, astfel încât acestea din urmă să efectueze, dacă împărtășesc îndoielile acestei autorități în ceea ce privește validitatea deciziei privind caracterul adecvat al nivelului de protecție, o trimitere preliminară în vederea examinării acestei validități."

[16] Atunci când se evaluează cadrul juridic al țării terțe, ar trebui să se ia în considerare posibilitatea ca pedeapsa cu moartea sau orice formă de tratament crud și inuman să fie impusă pe baza datelor transferate din UE. Într-adevăr, în cazul în care legislația țării terțe respective prevede o astfel de pedeapsă sau un astfel de tratament, ar trebui să se găsească garanții suplimentare în cadrul juridic al țării terțe pentru a se asigura că datele transferate din UE nu vor fi utilizate pentru a solicita, a pronunța sau a executa o pedeapsă cu moartea sau orice altă formă de tratament crud și inuman (de exemplu, un acord internațional care să impună condiții privind transferul, un angajament al țării terțe de a nu impune pedeapsa cu moartea sau orice formă de tratament crud și inuman pe baza datelor transferate din UE sau un moratoriu privind pedeapsa cu moartea).

funcționarea efectivă a uneia sau mai multor autorități de supraveghere independente și angajamentele internaționale la care a aderat țara terță sau organizația internațională.

25. Prin urmare, este clar că orice analiză pertinentă a nivelului adecvat de protecție trebuie să cuprindă cele două elemente fundamentale: conținutul normelor aplicabile și mijloacele pentru asigurarea aplicării efective a acestora. Comisiei Europene îi revine sarcina de a verifica, în mod regulat, eficacitatea în practică a normelor în vigoare.

26. Nucleul principiilor generale de protecție a datelor și al cerințelor procedurale și de asigurare a respectării legii, care ar putea fi considerate o cerință minimă pentru o protecție adecvată, derivă din Carta drepturilor fundamentale a UE (denumită în continuare „carta") și din LED. Nu este suficientă existența unor dispoziții generale privind protecția datelor și a vieții private în țara terță în cauză. Dimpotrivă, în cadrul juridic al țării terțe sau al organizației internaționale trebuie incluse dispoziții specifice care să abordeze în mod concret dreptul la protecția datelor în domeniul asigurării respectării legii. Țara terță ar trebui să ofere garanții care să asigure un nivel adecvat de protecție, în esență echivalent cu cel asigurat în cadrul Uniunii. Aceste dispoziții trebuie să fie executorii.

27. În plus, în ceea ce privește principiul proporționalității[17], CJUE a statuat, în legătură cu legislațiile statelor membre, că trebuie să se aprecieze dacă o restrângere a dreptului la viață privată și la protecția datelor poate fi justificată, pe de o parte, prin măsurarea **gravității ingerinței** pe care o implică o astfel de restrângere[18] și prin verificarea proporționalității **importanței obiectivului de interes general** urmărit de această limitare, pe de altă parte[19].

28. Potrivit jurisprudenței CJUE, un temei juridic care permite ingerința în drepturile fundamentale trebuie, pentru a îndeplini cerințele principiului proporționalității, să definească el însuși întinderea restrângerii exercitării dreptului vizat[20]. Derogările de la protecția datelor cu caracter personal și restrângerile acesteia trebuie să fie efectuate în limitele strictului necesar[21]. Pentru a îndeplini această cerință, pe lângă stabilirea unor norme clare și precise care să reglementeze domeniul de aplicare și aplicarea măsurii respective, legislația în cauză trebuie să impună garanții minime, astfel încât persoanele ale căror date au fost transferate să dispună de garanții suficiente pentru a-și proteja în mod eficient datele cu caracter personal împotriva riscului de abuz. „Această reglementare trebuie în special să indice în ce împrejurări și în ce condiții poate fi luată o măsură care prevede prelucrarea unor asemenea date, garantând în acest mod că o ingerință este limitată la strictul necesar. Necesitatea de a dispune de astfel de garanții este cu atât mai importantă atunci când datele cu caracter personal sunt supuse unei prelucrări automatizate."[22]

29. CEPD a adoptat recomandări care identifică garanții esențiale care reflectă jurisprudența CJUE și a Curții Europene a Drepturilor Omului (CEDO) în domeniul supravegherii și care trebuie să se regăsească în legislația țării terțe atunci când se evaluează ingerința măsurilor de supraveghere ale unei țări terțe în drepturile persoanelor vizate în cazul în care datele sunt transferate către

[17] Articolul 52 alineatul (1) din cartă.
[18] Instanța a arătat, de exemplu, că „ingerința pe care o presupune colectarea în timp real a datelor care permit localizarea unui echipament terminal este deosebit de gravă, din moment ce aceste date furnizează autorităților naționale competente mijlocul unei monitorizări precise și permanente a deplasărilor utilizatorilor de telefoane mobile (...)" (cauzele conexate C-511/18, C-512/18 și C-520/18, La Quadrature du Net și alții, 6 octombrie 2020, ECLI:EU:C:2020:791, punctul 187, inclusiv jurisprudența citată).
[19] La Quadrature du Net și alții, punctul 131.
[20] Schrems II, punctul 180.
[21] Schrems II, punctul 176, inclusiv jurisprudența citată.
[22] Schrems II, punctul 176, inclusiv jurisprudența citată.

țara terță respectivă în temeiul RGPD[23]. Pentru a evalua dacă sunt îndeplinite condițiile prevăzute la articolul 36 alineatul (2) litera (a) din LED, CEPD consideră că garanțiile prevăzute în aceste recomandări trebuie să fie luate în considerare atunci când se evaluează caracterul adecvat al nivelului de protecție al unei țări terțe în temeiul LED în domeniul supravegherii, ținând seama de alte condiții specifice în domeniul supravegherii în acest context.

30. În ceea ce privește cerința de la articolul 36 alineatul (2) litera (b), țara terță ar trebui nu numai să asigure o supraveghere efectivă independentă în materie de protecție a datelor, ci și să prevadă mecanisme de cooperare cu autoritățile de protecție a datelor din statele membre[24].

31. În ceea ce privește cerința de la articolul 36 alineatul (2) litera (c), pe lângă angajamentele internaționale asumate de țara terță sau de organizația internațională, ar trebui să se țină seama și de obligațiile care decurg din participarea țării terțe sau a organizației internaționale la sistemele multilaterale sau regionale, în special în ceea ce privește protecția datelor cu caracter personal, precum și de punerea în aplicare a unor astfel de obligații, în special aderarea țării terțe la alte acorduri internaționale privind protecția datelor cu caracter personal, cum ar fi Convenția Consiliului Europei din 28 ianuarie 1981 pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal și protocolul adițional la aceasta (Convenția 108[25] și versiunea modernizată a acesteia, Convenția 108+). Respectarea de către țara terță a principiilor consacrate în documente internaționale, cum ar fi Ghidul practic al Consiliului Europei privind utilizarea datelor cu caracter personal în sectorul polițienesc: se poate lua în considerare și modul de protejare a datelor cu caracter personal în paralel cu combaterea criminalității.

32. O decizie privind caracterul adecvat al nivelului de protecție ar trebui să garanteze că, prin conținutul drepturilor la viață privată și la protecția datelor și prin punerea în aplicare, supravegherea și asigurarea respectării lor efective, sistemul străin în ansamblul său asigură nivelul necesar de protecție, inclusiv pentru datele în tranzit către această țară terță. Astfel cum a subliniat CJUE în hotărârea Schrems II, nivelul ridicat de protecție acordat ar trebui să fie asigurat și în cursul transferării datelor către o țară terță[26].

33. În cele din urmă, atunci când adoptă o decizie privind caracterul adecvat al nivelului de protecție doar pentru un teritoriu sau un sector specificat dintr-o țară terță, Comisia Europeană ar trebui să țină seama de criterii clare și obiective, cum ar fi activitățile specifice de prelucrare sau domeniul de aplicare al standardelor juridice aplicabile și legislația în vigoare în țara terță respectivă[27].

A. Principii generale și garanții

a) Concepte

34. Ar trebui să existe concepte de bază în materie de protecție a datelor. Nu este necesar ca ele să corespundă întocmai terminologiei LED, dar ar trebui să reflecte conceptele consacrate în legislația europeană privind protecția datelor și să fie în concordanță cu acestea. De exemplu, LED include următoarele concepte importante: „date cu caracter personal”, „prelucrarea datelor cu caracter personal”, „autorități competente”, „operator de date”, „persoană împuternicită de

[23] Recomandările 02/2020 ale CEPD privind garanțiile esențiale europene pentru măsurile de supraveghere, adoptate la 10 noiembrie 2020.
[24] Considerentul 67 din LED.
[25] Considerentul 68 din LED.
[26] A se vedea punctul 93.
[27] Considerentul 67 din LED.

operator", „destinatar", „date sensibile", „exactitate", „creare de profiluri", „asigurarea protecției datelor începând cu momentul conceperii și în mod implicit", „autoritate de supraveghere" și „pseudonimizare".

b) Legalitatea și echitatea prelucrării datelor cu caracter personal (articolul 4 - considerentul 26)

35. Potrivit articolului 8 alineatul (2) din cartă, datele cu caracter personal ar trebui, printre altele, să fie prelucrate „în scopurile precizate și pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege"[28]. Totuși, în contextul asigurării respectării legii, ar trebui remarcat faptul că îndeplinirea sarcinilor de prevenire, investigare, depistare sau urmărire penală a infracțiunilor, conferite instituțional prin lege autorităților competente, le permite acestora să solicite sau să dispună ca persoanele fizice să se conformeze cererilor formulate. În acest caz, consimțământul persoanei vizate nu ar trebui să constituie un temei juridic pentru prelucrarea datelor cu caracter personal de către autoritățile competente[29].

36. Acest temei juridic ar trebui să stabilească norme clare și precise care să reglementeze conținutul și aplicarea activităților relevante de prelucrare a datelor și să impună o serie de cerințe minime[30]. În plus, CJUE a reamintit că „reglementarea trebuie să fie obligatorie din punct de vedere juridic în dreptul intern"[31].

37. Pentru a fi legală, prelucrarea datelor[32] ar trebui să fie necesară pentru îndeplinirea unei sarcini de către o autoritate competentă în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora[33]. Aceste scopuri ar trebui prevăzute în legislația națională.

38. Datele cu caracter personal trebuie să fie prelucrate în mod echitabil. Principiul prelucrării echitabile a datelor din domeniul protecției datelor cu caracter personal este o noțiune distinctă de dreptul la un proces echitabil, astfel cum este definit la articolul 47 din cartă și la articolul 6 din Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale (CEDO)[34].

c) Principiul limitării scopului (articolul 4)

[28] A se vedea Schrems II, punctul 173.

[29] Considerentul 35 din LED afirmă și că „[î]n cazul în care i se solicită persoanei vizate să respecte o obligație legală, persoana vizată nu dispune cu adevărat de libertatea de alegere, astfel încât reacția persoanei vizate nu poate fi considerată ca o manifestare liberă a voinței sale. Acest lucru nu ar trebui să împiedice statele membre să prevadă prin lege că persoana vizată poate accepta prelucrarea datelor sale cu caracter personal în scopurile prezentei directive, cum ar fi testele ADN în anchetele penale sau monitorizarea localizării persoanei vizate prin dispozitive electronice pentru executarea pedepselor."

[30] A se vedea Schrems II, punctele 175 și 180 și Avizul 1/15, punctul 139 și jurisprudența citată.

[31] A se vedea cauza C-623/17, Privacy International/Secretary of State for Foreign and Commonwealth Affairs și alții, 6 octombrie 2020, ECLI:EU:C:2020:790, punctul 68 - De asemenea, ar trebui să fie clarificat faptul că, în versiunea în limba franceză a hotărârii, CJUE utilizează termenul „*réglementation*", care are un sens mai larg, nu se referă doar la actele Parlamentului.

[32] Prelucrarea datelor cu caracter personal, efectuată total sau parțial prin mijloace automatizate, precum și prelucrarea prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență sau care sunt destinate să facă parte dintr-un sistem de evidență.

[33] Autoritățile competente sunt orice autoritate publică competentă în acest sens sau orice alt organism sau entitate împuternicită prin lege să exercite autoritate publică și competențe publice în acest scop.

[34] Considerentul 26 din LED.

39. Scopurile specifice în care datele cu caracter personal sunt prelucrate ar trebui să fie explicite și legitime și să fie determinate la momentul colectării datelor[35].

40. Datele ar trebui prelucrate în scopuri determinate, explicite și legitime în cadrul obiectivelor prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor[36], inclusiv al protejării împotriva amenințărilor la adresa securității publice din țara terță și al prevenirii acestora, și ar trebui utilizate ulterior în oricare dintre aceste scopuri, în măsura în care acest lucru nu este incompatibil cu scopul inițial al prelucrării (de exemplu, pentru proceduri paralele de asigurare a respectării legii sau pentru arhivarea în interes public sau în scopuri științifice, statistice sau istorice) și sub rezerva unor garanții adecvate pentru drepturile și libertățile persoanelor vizate. În cazul în care datele cu caracter personal sunt prelucrate de același operator sau de un alt operator (autoritatea competentă[37]) în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau al executării pedepselor, altul decât cel pentru care au fost colectate, o astfel de prelucrare ar trebui să fie permisă cu condiția ca prelucrarea să fie autorizată în conformitate cu dispozițiile legale aplicabile și să fie necesară și proporțională cu acest alt scop[38]. De asemenea, ar trebui să se ia în considerare existența unui mecanism de informare a autorităților competente relevante ale statelor membre cu privire la o astfel de prelucrare ulterioară a datelor[39]. În plus, în orice caz, nivelul de protecție a persoanelor fizice în Uniune prevăzut de LED nu ar trebui să fie diminuat, inclusiv în cazurile în care datele cu caracter personal sunt transmise din țara terță către operatori sau persoane împuternicite de operatori din aceeași țară terță[40].

d) Condiții specifice pentru prelucrarea ulterioară în alte scopuri (articolul 9)

41. În ceea ce privește prelucrarea sau divulgarea ulterioară a datelor transferate din UE în alte scopuri decât cele de asigurare a respectării legii, cum ar fi scopurile legate de securitatea națională, aceasta ar trebui, de asemenea, să fie prevăzută de lege, să fie necesară și proporțională. De asemenea, ar trebui să se ia în considerare existența unui mecanism de informare a autorităților competente relevante ale statelor membre cu privire la o astfel de prelucrare ulterioară a datelor[41]. Și în acest caz, după prelucrarea sau divulgarea ulterioară, datele ar trebui să beneficieze de același nivel de protecție ca atunci când au fost prelucrate inițial de autoritatea competentă destinatară.

e) Principiul reducerii la minimum a datelor

[35] Considerentul 26 din LED.
[36] Aceasta include „activitățile polițienești desfășurate fără a cunoaște dinainte dacă un incident constituie o infracțiune. Activitățile respective pot include, de asemenea, exercitarea autorității prin aplicarea unor măsuri coercitive, precum activitățile polițienești desfășurate cu ocazia unor manifestații, evenimente sportive majore și revolte. De asemenea, activitățile menționate includ menținerea legii și ordinii ca atribuții ale poliției sau ale altor autorități de aplicare a legii atunci când aceasta se impune pentru a se asigura protecția împotriva amenințărilor la adresa securității publice și la adresa intereselor fundamentale ale societății protejate prin lege și pentru prevenirea acestor amenințări, care pot conduce la o infracțiune." (considerentul 12 din LED) Trebuie făcută distincția între acestea și scopul securității naționale sau activitățile care intră sub incidența capitolului 2 din titlul V din Tratatul privind Uniunea Europeană (TUE) (considerentul 14 din LED).
[37] A se vedea nota de subsol 33.
[38] Considerentul 29 din LED.
[39] Un astfel de mecanism ar putea consta, de exemplu, în coduri de utilizare convenite de comun acord, într-o obligație de notificare în temeiul unui instrument internațional, inclusiv eventualele notificări automatizate, sau în alte măsuri similare de asigurare a transparenței.
[40] Considerentul 64 din LED.
[41] A se vedea nota de subsol 39.

42. Datele ar trebui să fie adecvate și relevante și să nu fie excesive în raport cu scopurile în care sunt prelucrate. În special, ar trebui să se ia în considerare aplicarea unor cerințe privind protecția datelor începând cu momentul conceperii și protecția implicită a datelor, cum ar fi câmpuri de intrare limitate (comunicațiile structurate) sau verificări de calitate automatizate și neautomatizate.

f) Principiul exactității datelor

43. Datele ar trebui să fie exacte și, dacă este necesar, actualizate. Cu toate acestea, principiul exactității datelor ar trebui aplicat luând în considerare natura și scopul prelucrării în cauză. În special în cadrul procedurilor judiciare, declarațiile care conțin date cu caracter personal se bazează pe o percepție subiectivă a persoanelor fizice și nu sunt întotdeauna verificabile. În consecință, acest principiu nu ar trebui să se aplice exactității unei declarații, ci doar faptului că o anumită declarație a fost făcută[42].

44. Ar trebui să se asigure faptul că datele cu caracter personal care sunt inexacte, incomplete sau nu mai sunt actuale nu sunt transmise sau puse la dispoziție[43] și că sunt prevăzute proceduri pentru corectarea sau ștergerea datelor inexacte. În special, ar trebui să se ia în considerare orice sistem de clasificare a informațiilor prelucrate, în ceea ce privește fiabilitatea sursei și nivelul de verificare a faptelor[44].

g) Principiul păstrării datelor

45. Datele nu ar trebui păstrate mai mult decât este necesar pentru scopurile în care sunt prelucrate. Ar trebui instituite mecanisme adecvate pentru ștergerea datelor cu caracter personal; acestea pot consta într-o perioadă fixă sau o revizuire periodică a necesității de stocare a datelor cu caracter personal (sau o combinație a celor două: perioadă maximă fixă și revizuire periodică la anumite intervale)[45]. Datele cu caracter personal care sunt stocate pe o perioadă mai lungă, în scopuri de arhivare în interes public sau în scopuri științifice, statistice sau istorice ar trebui să facă obiectul unor garanții adecvate (de exemplu, în ceea ce privește accesul)[46].

h) Principiul securității și confidențialității (articolul 29, considerentele 28 și 71)

46. Orice entitate care prelucrează date cu caracter personal ar trebui să se asigure că datele sunt prelucrate într-un mod care să asigure securitatea acestora, inclusiv prin prevenirea accesului neautorizat sau a utilizării neautorizate a datelor cu caracter personal și a echipamentelor utilizate pentru prelucrare. Aceasta include protecția împotriva prelucrării ilegale, precum și împotriva pierderii, distrugerii sau deteriorării accidentale, prin intermediul unor măsuri tehnice și organizatorice adecvate, precum și adoptarea unor măsuri corespunzătoare. Atunci când se stabilește nivelul de securitate, ar trebui să se țină seama de stadiul actual al tehnologiei, de costurile punerii în aplicare și de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile la adresa drepturilor și libertăților persoanelor fizice, prezentând grade diferite de probabilitate și gravitate.

47. Ar trebui asigurate canale sigure de comunicare între autoritățile statelor membre care transferă datele cu caracter personal și autoritățile destinatare din statele terțe.

[42] Considerentul 30 din LED.
[43] Considerentul 32 din LED.
[44] De exemplu, grile 4x4 pentru evaluarea fiabilității și coduri de utilizare.
[45] Articolul 5 din LED.
[46] Considerentul 26 din LED.

i) Principiul transparenței (articolul 13, considerentele 26, 39, 42, 43, 44 și 46)

48. Persoanele fizice ar trebui să fie informate cu privire la riscurile, normele, garanțiile și drepturile în materie de prelucrare a datelor acestora cu caracter personal și cu privire la modul în care să își exercite drepturile respective[47].

49. Informațiile privind toate elementele principale ale prelucrării datelor lor cu caracter personal ar trebui puse la dispoziția persoanelor fizice. Aceste informații ar trebui să fie ușor accesibile și ușor de înțeles, utilizând un limbaj clar și simplu. Astfel de informații ar trebui să includă scopul prelucrării, identitatea operatorului de date, drepturile de care dispun[48] și alte informații în măsura în care acest lucru este necesar pentru a asigura o procedură echitabilă.

50. Pot exista unele excepții de la acest drept la informare. Totuși, o astfel de limitare ar trebui să fie permisă printr-o măsură legislativă și să fie necesară și proporțională pentru a evita obstrucționarea anchetelor, investigațiilor sau procedurilor oficiale sau juridice, pentru a evita prejudicierea prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau a executării pedepselor, pentru a proteja siguranța publică sau securitatea națională sau pentru a proteja drepturile și libertățile altora, atât timp cât o astfel de restricție parțială sau totală constituie o măsură necesară și proporțională într-o societate democratică, ținând seama în mod corespunzător de drepturile fundamentale și de interesele legitime ale persoanei fizice în cauză. Astfel de restricționări ar trebui, de asemenea, să fie luate în considerare și evaluate ținând seama de posibilitatea de a depune o plângere la o autoritate de supraveghere sau de a introduce o cale de atac. În orice caz, orice restricție posibilă ar trebui să fie temporară și nu generală și ar trebui să fie încadrată în condiții, garanții și limitări similare celor impuse de cartă și de CEDO, astfel cum sunt interpretate de jurisprudența CJUE și, respectiv, a Curții Europene a Drepturilor Omului, și, în special, să respecte esența drepturilor și libertăților respective.

j) Dreptul de acces, de rectificare și de ștergere (articolele 14 și 16)

51. Persoana vizată ar trebui să aibă dreptul de a obține o confirmare că se prelucrează sau nu date care o privesc și, în caz afirmativ, să aibă acces la datele sale. Acest drept ar trebui să cuprindă cel puțin anumite informații cu privire la prelucrare, cum ar fi scopul și temeiul juridic al prelucrării, dreptul de a depune o plângere la autoritatea de supraveghere sau categoriile de date cu caracter personal vizate[49]. Acest lucru este deosebit de important în cazul în care transparența se realizează prin intermediul unui anunț general (de exemplu, informații pe site-ul autorității).

52. Persoana vizată ar trebui să aibă dreptul de a obține rectificarea datelor sale din motive specificate, de exemplu, în cazul în care se dovedește că acestea sunt inexacte sau incomplete. De asemenea, persoana vizată ar trebui să aibă dreptul de a obține ștergerea datelor sale atunci când, de exemplu, prelucrarea acestora nu mai este necesară sau este ilegală.

53. Exercitarea acestor drepturi nu ar trebui să fie excesiv de împovărătoare pentru persoana vizată.

k) Restricționări ale drepturilor persoanelor vizate

54. Ar putea exista eventuale restricționări ale acestor drepturi pentru a evita obstrucționarea anchetelor, cercetărilor sau procedurilor oficiale sau judiciare, pentru a evita prejudicierea

[47] Considerentul 26 din LED.
[48] Atât drepturile materiale (dreptul de acces, de rectificare etc.), cât și dreptul la reparații.
[49] Articolul 14 din LED.

prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau a executării pedepselor, pentru a proteja siguranța publică sau securitatea națională sau pentru a proteja drepturile și libertățile altora, atât timp cât o astfel de restricționare parțială sau totală constituie o măsură necesară și proporțională într-o societate democratică, ținând seama în mod corespunzător de drepturile fundamentale și de interesele legitime ale persoanei fizice în cauză. Astfel de restricționări ar trebui, de asemenea, să fie luate în considerare și evaluate ținând seama de posibilitatea de a depune o plângere la o autoritate de supraveghere sau de a introduce o cale de atac.

l) Restricționarea transferurilor ulterioare (articolul 35, considerentele 64-65)

55. Transferurile ulterioare de date cu caracter personal de către destinatarul inițial către o altă țară terță sau organizație internațională nu trebuie să diminueze nivelul de protecție, prevăzut în Uniune, al persoanelor fizice ale căror date sunt transferate. Prin urmare, astfel de transferuri ulterioare de date ar trebui să fie permise numai în cazul în care este asigurată continuitatea nivelului de protecție prevăzut de legislația UE[50]. În special, destinatarul suplimentar (și anume destinatarul transferului ulterior) ar trebui să fie o autoritate competentă în scopul asigurării respectării legii[51], iar astfel de transferuri ulterioare de date pot avea loc numai în scopuri limitate și determinate și atât timp cât există un temei juridic pentru prelucrarea respectivă.

56. De asemenea, trebuie să se ia în considerare existența unui mecanism prin care autoritățile competente relevante ale statului membru să fie informate și să autorizeze un astfel de transfer ulterior de date. Destinatarul inițial al datelor transferate din UE ar trebui să fie responsabil și să fie în măsură să demonstreze că autoritatea competentă relevantă a statului membru a autorizat transferul ulterior[52] și că sunt prevăzute garanții adecvate pentru transferurile ulterioare de date în absența unei decizii privind caracterul adecvat al nivelului de protecție referitoare la țara terță către care datele ar urma să fie transferate ulterior[53].

m) Principiul responsabilității [articolul 4 alineatul (4)]

57. Operatorul ar trebui să fie responsabil și să fie în măsură să demonstreze respectarea principiilor de protecție a datelor prevăzute la articolul 4 din LED.

[50] A se vedea și Avizul 1/15.
[51] A se vedea nota de subsol 33.
[52] În acest context, ar trebui să ia în considerare existența unei obligații sau a unui angajament de a pune în aplicare codurile de utilizare relevante definite de autoritățile statelor membre care efectuează transferul.
[53] Cerințele de mai sus nu aduc atingere condițiilor specifice pentru transferurile ulterioare către o țară adecvată stabilite în temeiul LED [articolul 35 alineatul (1) literele (c) și (e)].

B. Exemple de principii suplimentare care trebuie aplicate unor tipuri specifice de prelucrare

a) Categorii speciale de date (articolul 10 și considerentul 37)

58. Ar trebui să existe garanții specifice în cazul în care sunt implicate „categorii speciale de date”[54], abordând riscurile specifice implicate[55]. Aceste categorii ar trebui să le reflecte pe cele prevăzute la articolul 10 din LED. Prelucrarea categoriilor speciale de date ar trebui, prin urmare, să facă obiectul unor garanții specifice și să fie permisă numai în cazul în care acest lucru este strict necesar în anumite condiții, de exemplu pentru a proteja interesul vital al unei persoane.

b) Procesul decizional automatizat și crearea de profiluri (articolul 11 și considerentul 38)

59. Deciziile bazate exclusiv pe prelucrarea automatizată (procesul decizional individual automatizat), inclusiv crearea de profiluri, care produc efecte juridice sau care afectează în mod semnificativ persoana vizată pot avea loc numai în anumite condiții stabilite în cadrul juridic al țării terțe[56].

60. În cadrul Uniunii, astfel de condiții includ, de exemplu, furnizarea de informații specifice persoanei vizate și dreptul de a obține intervenția umană din partea operatorului, în special de a-și exprima punctul de vedere, de a obține o explicație cu privire la decizia luată în urma unei astfel de evaluări sau de a contesta decizia.

61. Legislația țării terțe ar trebui, în orice caz, să prevadă garanțiile necesare pentru drepturile și libertățile persoanei vizate. În acest sens, ar trebui, de asemenea, să se ia în considerare existența unui mecanism de informare a autorităților competente relevante ale statelor membre cu privire la orice prelucrare ulterioară, cum ar fi utilizarea datelor transferate pentru crearea de profiluri la scară largă.

c) Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit (articolul 20)

62. Atunci când se evaluează caracterul adecvat al nivelului de protecție, ar trebui să se acorde atenție existenței unei obligații a operatorilor de a adopta politici interne și de a pune în aplicare măsuri care să respecte principiul protecției datelor începând cu momentul conceperii și al protecției implicite a datelor, ținând seama de stadiul actual al tehnologiei, de costul punerii în aplicare și de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile prelucrării la adresa drepturilor și libertăților persoanelor fizice, prezentând grade diferite de probabilitate și gravitate, atât în momentul stabilirii mijloacelor de prelucrare, cât și în momentul prelucrării efective, pentru a integra în mod adecvat măsuri de protecție a datelor, cum ar fi pseudonimizarea, care sunt menite să pună în aplicare principiile protecției datelor, cum ar fi reducerea la minimum a datelor, într-un mod eficient și pentru a integra garanții în cadrul prelucrării.

[54] Aceste categorii speciale sunt denumite și „date sensibile” în considerentul 37 din LED.
[55] Astfel de garanții suplimentare ar putea fi, de exemplu, măsuri de securitate specifice, drepturi limitate de acces pentru personal, restricții în ceea ce privește prelucrarea ulterioară, procesul decizional automatizat, partajarea ulterioară sau transferurile ulterioare.
[56] Avizul 1/15, punctul 173.

C. Mecanisme procedurale și de asigurare a respectării dispozițiilor

63. Chiar dacă mijloacele la care țara terță a recurs pentru a asigura un nivel adecvat de protecție pot fi diferite de cele puse în aplicare în cadrul Uniunii Europene[57], un sistem coerent cu cel european trebuie să fie caracterizat de existența următoarelor elemente:

a) Autoritatea de supraveghere independentă competentă [articolul 36 alineatul (2) litera (b), articolul 36 alineatul (3) și considerentul 67]

64. Ar trebui să existe una sau mai multe autorități de supraveghere independente, însărcinate cu monitorizarea, asigurarea și impunerea respectării dispozițiilor privind protecția datelor și a vieții private în țara terță. Autoritatea de supraveghere beneficiază de independență și imparțialitate deplină în îndeplinirea sarcinilor sale și în exercitarea competențelor sale și, în acest sens, nu solicită și nici nu acceptă instrucțiuni. În acest context, autoritatea de supraveghere ar trebui să dispună de toate competențele adecvate de aplicare a legii pentru a asigura în mod eficace respectarea drepturilor în materie de protecție a datelor și pentru a promova sensibilizarea. Ar trebui să se acorde atenție și personalului și bugetului autorității de supraveghere. De asemenea, autoritatea de supraveghere poate, din proprie inițiativă, să efectueze investigații. Aceasta ar trebui, de asemenea, să aibă sarcina de a asista și de a consilia persoanele vizate în exercitarea drepturilor lor [a se vedea și litera (c) de mai jos]. Deciziile privind caracterul adecvat al nivelului de protecție ar trebui să identifice autoritatea sau, după caz, autoritățile de supraveghere respective și mecanismele de cooperare cu autoritățile de supraveghere din statele membre pentru a asigura respectarea normelor privind protecția datelor.

b) Punerea efectivă în aplicare a normelor privind protecția datelor

65. Sistemul unei țări terțe ar trebui să asigure un nivel ridicat de responsabilitate și de sensibilizare în rândul operatorilor de date și al celor care prelucrează datele cu caracter personal în numele acestora cu privire la obligațiile, sarcinile și responsabilitățile care le revin, precum și în rândul persoanelor vizate cu privire la drepturile lor și la mijloacele de exercitare a acestora. Existența unor sancțiuni eficace și disuasive poate juca un rol important în asigurarea respectării normelor, ca și sistemele de verificare directă de către autorități, auditori sau funcționari independenți însărcinați cu protecția datelor.

66. Cadrul de protecție a datelor al unei țări terțe ar trebui să oblige operatorii de date și/sau pe cei care prelucrează datele cu caracter personal în numele acestora să îl respecte și să fie în măsură să își demonstreze conformitatea în special în fața autorității de supraveghere competente. Astfel de măsuri ar trebui să includă păstrarea înregistrărilor sau a fișierelor-jurnal ale activităților de prelucrare a datelor pentru o perioadă de timp adecvată. Acestea pot include, de exemplu, evaluări ale impactului asupra protecției datelor, desemnarea unui responsabil cu protecția datelor sau protecția datelor începând cu momentul conceperii și protecția implicită a datelor.

c) Sistemul de protecție a datelor trebuie să faciliteze exercitarea drepturilor persoanelor vizate (articolele 12, 17 și 46 din LED)

67. Un cadru de protecție a datelor dintr-o țară terță ar trebui să oblige operatorii de date să faciliteze exercitarea drepturilor persoanelor vizate menționate în secțiunea A litera (j) de mai sus și să

[57] Schrems I, punctul 74.

prevadă că autoritatea sa de supraveghere, la cerere, informează orice persoană vizată cu privire la exercitarea drepturilor sale[58].

d) Sistemul de protecție a datelor trebuie să ofere căi de atac adecvate

68. Deși în prezent nu există jurisprudență cu privire la caracterul adecvat al nivelului de protecție oferit de sistemul juridic al unei țări terțe în temeiul LED, CJUE a interpretat dreptul fundamental la protecție jurisdicțională efectivă, astfel cum este consacrat la articolul 47 din cartă. Astfel, articolul 47 primul paragraf din cartă prevede că orice persoană ale cărei drepturi și libertăți garantate de dreptul Uniunii sunt încălcate are dreptul la o cale de atac eficientă în fața unei instanțe judecătorești[59], în conformitate cu condițiile stabilite de articolul respectiv.

69. În conformitate cu jurisprudența constantă a CJUE, însăși existența unui control jurisdicțional efectiv menit să asigure conformitatea cu dispozițiile dreptului UE este inerentă existenței statului de drept. Astfel, o reglementare care nu prevede nicio posibilitate prin care o persoană să exercite căi de atac pentru a avea acces la datele cu caracter personal care o privesc sau pentru a obține rectificarea sau ștergerea unor astfel de date contravine esenței dreptului fundamental la protecție jurisdicțională efectivă, astfel cum este consacrat la articolul 47 din cartă[60].

70. Fiecare persoană ar trebui să aibă posibilitatea de a acționa pentru a-și exercita drepturile în mod rapid și eficace, fără costuri prohibitive, precum și de a asigura respectarea acestora.

71. În acest scop, trebuie să existe mecanisme de supraveghere care să permită investigarea independentă a plângerilor și identificarea și sancționarea în practică a tuturor încălcărilor dreptului la protecția datelor și la respectarea vieții private.

72. În cazul în care normele nu sunt respectate, persoana vizată ale cărei date cu caracter personal sunt transferate către o țară terță ar trebui să beneficieze de căi de atac administrative și judiciare eficace în țara terță respectivă, inclusiv cu privire la despăgubiri pentru prejudiciile cauzate de prelucrarea ilegală a datelor sale cu caracter personal. Acesta este un element esențial care trebuie să implice un sistem independent de adjudecare sau arbitraj care să permită plata de despăgubiri și impunerea de sancțiuni, după caz.

[58] Exercitarea drepturilor persoanelor vizate ar putea fi directă sau indirectă.
[59] CJUE consideră că o protecție jurisdicțională efectivă poate fi asigurată nu numai de o instanță, ci și de un organism care oferă garanții echivalente în esență cu cele prevăzute la articolul 47 din cartă (a se vedea Schrems II, punctul 197). Acest lucru ar putea fi relevant în special pentru organizațiile internaționale.
[60] Schrems II, punctele 187 și 194, inclusiv jurisprudența citată.