Avizul 15/2021 referitor la proiectul de decizie de punere în aplicare a Comisiei Europene în temeiul Directivei (UE) 2016/680 privind protecția adecvată a datelor cu caracter personal în Regatul Unit al Marii Britanii și Irlandei de Nord

Adoptat la 13 aprilie 2021

Istoricul versiunilor

Versiunea 1.1	6 iulie 2021	Schimbări legate de formatare
Versiunea 1.0	13 aprilie 2021	Adoptarea avizului

CUPRINS

Comitetul european pentru protecția datelor (CEPD)

având în vedere articolul 51 alineatul (1) litera (g) 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] (denumită în continuare „LED"),

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

ADOPTĂ PREZENTUL AVIZ:

1 REZUMAT

1. La 19 februarie 2021, Comisia Europeană a aprobat proiectul său de decizie de punere în aplicare (denumit în continuare „proiectul de decizie") privind nivelul adecvat de protecție a datelor cu caracter personal asigurat de Regatul Unit al Marii Britanii și Irlandei de Nord (denumit în continuare „Regatul Unit") în temeiul LED[2]. Ulterior, Comisia Europeană a lansat procedura pentru adoptarea formală a acestuia.

2. La aceeași dată, Comisia Europeană a solicitat avizul Comitetului european pentru protecția datelor (denumit în continuare „CEPD")[3]. Evaluarea CEPD cu privire la caracterul adecvat al nivelului de protecție asigurat în Regatul Unit a fost efectuată pe baza examinării proiectului de decizie, precum și pe baza unei analize a documentației puse la dispoziție de Comisia Europeană.

3. În acest demers, CEPD a folosit ca referință principală criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul LED[4], adoptate la 2 februarie 2021, precum și jurisprudența relevantă reflectată în Recomandările 02/2020 ale CEPD privind garanțiile esențiale europene pentru măsurile de supraveghere[5].

4. Obiectivul principal urmărit de CEPD este de a emite un aviz pentru Comisia Europeană cu privire la caracterul adecvat al nivelului de protecție oferit persoanelor fizice în Regatul Unit. Este important să se recunoască faptul că CEPD nu se așteptă să aibă loc o reproducere a legislației europene privind protecția datelor în cadrul juridic aplicat în Regatul Unit.

[1] JO L 119, 4.5.2016, p. 89.
[2] A se vedea comunicatul de presă al Comisiei Europene, comunicat de presă, Protecția datelor: Comisia Europeană lansează procesul privind fluxurile de date cu caracter personal către Regatul Unit, 19 februarie 2021, https://ec.europa.eu/commission/presscorner/detail/ro/ip_21_661.
[3] Idem.
[4] A se vedea Recomandările CEPD 01/2021 cu privire la criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul Directivei privind protecția datelor în materie de aplicare a legii, adoptate la 2 februarie 2021, https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_ro.pdf.
[5] A se vedea Recomandările CEPD 02/2020 privind garanțiile esențiale europene pentru măsurile de supraveghere, adoptate la 10 noiembrie 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_ro.pdf.

5. Cu toate acestea, CEPD reamintește faptul că, în conformitate cu articolul 36 din LED și cu jurisprudența Curții de Justiție a Uniunii Europene (denumită în continuare „CJUE"), se consideră că legislația unei țări terțe oferă un nivel adecvat de protecție atunci când legislația respectivă este aliniată la esența principiilor fundamentale consacrate în LED. În ceea ce privește protecția datelor, CEPD constată că există o strânsă aliniere între cadrul prevăzut în LED și cadrul juridic al Regatului Unit cu privire la anumite dispoziții esențiale, cum ar fi: concepte (de exemplu, „date cu caracter personal"; „prelucrarea datelor cu caracter personal"; „operator"); motive care justifică prelucrarea legală și echitabilă în scopuri legitime; limitarea scopului; calitatea și proporționalitatea datelor; păstrarea, securitatea și confidențialitatea datelor; transparența; categoriile speciale de date; procesul decizional automatizat și crearea de profiluri.

6. CEPD recomandă Comisiei Europene să își completeze analiza cu informații privind existența unui mecanism de informare a autorităților competente relevante ale statelor membre cu privire la prelucrarea sau divulgarea ulterioară a datelor de către autoritățile Regatului Unit cărora respectivele autorități competente ale statelor membre le-au transferat datele cu caracter personal și să identifice eficacitatea acestui mecanism în temeiul ordinii juridice a Regatului Unit.

7. CEPD consideră că dispozițiile din capitolul 5 al părții 3 din Legea privind protecția datelor din 2018 (denumită în continuare „DPA 2018"), reușesc, în principiu, să asigure un nivel de protecție care este în esență echivalent cu cel garantat în temeiul dreptului UE în ceea ce privește transferul de date cu caracter personal de la o autoritate de aplicare a legii a Regatului Unit către o țară terță.

8. Deși CEPD ia act de capacitatea Regatului Unit, în temeiul cadrului său juridic, de a recunoaște că teritoriile oferă un nivel adecvat de protecție a datelor în conformitate cu cadrul de protecție a datelor aplicat în Regatul Unit, CEPD dorește să sublinieze că acest lucru ar putea conduce la posibile riscuri în ceea ce privește protecția oferită datelor cu caracter personal transferate din EU, în special în cazul în care, în viitor, cadrul de protecție a datelor aplicat în Regatul Unit se abate de la acquis-ul UE. **Prin urmare, în ceea ce privește situațiile de mai sus, Comisia Europeană ar trebui să își îndeplinească rolul de monitorizare, și, în cazul în care nu se menține nivelul în esență echivalent de protecție a datelor cu caracter personal transferate din UE, Comisia Europeană ar trebui să aibă în vedere modificarea deciziei privind caracterul adecvat al nivelului de protecție în sensul introducerii unor garanții specifice pentru datele transferate din UE și/sau în sensul suspendării deciziei privind caracterul adecvat al nivelului de protecție.**

9. **În cele din urmă, referitor la acordurile internaționale încheiate între Regatul Unit și țări terțe,** Comisia Europeană este invitată să examineze interacțiunea dintre cadrul de protecție a datelor din Regatul Unit și angajamentele sale internaționale, în special pentru a asigura continuitatea nivelului de protecție în cazul în care datele cu caracter personal sunt transferate din UE în Regatul Unit în baza deciziei Regatului Unit privind caracterul adecvat al nivelului de protecție și apoi transferate mai departe către alte țări terțe. Comisia Europeană este invitată, de asemenea, să monitorizeze în permanență și să ia măsuri, dacă este necesar, în cazul în care încheierea de acorduri internaționale între Regatul Unit și țări terțe riscă să diminueze nivelul de protecție a datelor cu caracter personal asigurat în UE.

10. În acest sens, CEPD subliniază că intrarea în vigoare a Acordului încheiat între Regatul Unit și SUA privind accesul la datele electronice în scopul combaterii formelor grave de criminalitate (denumit în continuare „Acordul între Regatul Unit și SUA privind Legea CLOUD")[6] poate afecta transferurile

[6] A se vedea Acordul între Guvernul Regatului Unit al Marii Britanii și Irlandei de Nord și Guvernul Statelor Unite ale Americii privind accesul la datele electronice în scopul combaterii formelor grave de criminalitate, Washington DC, SUA, 3 octombrie 2019.

ulterioare de date de la autoritățile de aplicare a legii din Regatul Unit, în special cu privire la emiterea și transmiterea de ordine de tip instrument juridic în conformitate cu articolul 5 din Acordul între Regatul Unit și SUA privind Legea CLOUD.

11. CEPD recomandă, de asemenea, Comisiei Europene să monitorizeze în permanență dacă încheierea unor viitoare acorduri cu țări terțe în scopul cooperării în materie de aplicare a legii, prin care se asigură un temei juridic pentru transferul de date cu caracter personal către țările respective, ar putea afecta condițiile pentru schimbul ulterior de informații colectate, în special dacă dispozițiile acestor acorduri internaționale ar putea afecta aplicarea legislației Regatului Unit privind protecția datelor și ar putea prevedea limitări sau excepțări suplimentare în ceea ce privește utilizarea și divulgarea ulterioară a informațiilor colectate în străinătate în scopul aplicării legii. CEPD consideră că astfel de informații și de evaluări sunt esențiale pentru a permite o revizuire cuprinzătoare a nivelului de protecție oferit de cadrul legislativ și de practicile utilizate în Regatul Unit cu privire la divulgarea datelor la nivel transfrontalier.

2 INTRODUCERE

2.1 Cadrul de protecție a datelor din Regatul Unit

12. Cadrul de protecție a datelor din Regatul Unit se bazează în mare parte pe cadrul de protecție a datelor din UE [în special LED și Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date (denumit în continuare „RGPD")], situație care rezultă din faptul că Regatul Unit a fost stat membru al UE până la 31 ianuarie 2020. În plus, pe lângă faptul că descrie în detaliu transpunerea RGPD în dreptul Regatului Unit și acordarea de competențe autorității naționale de supraveghere a protecției datelor și stabilirea de obligații în sarcina acesteia, și anume Biroul Comisarului pentru informații din Regatul Unit (denumit în continuare „ICO"), DPA 2018, care a intrat în vigoare la 23 mai 2018 și a abrogat Legea Regatului Unit privind protecția datelor din 1998, transpune LED în partea 3.

13. Astfel cum se menționează în considerentul 12 din proiectul de decizie, Guvernul Regatului Unit a adoptat „European Union (Withdrawal) Act 2018" [Legea din 2018 privind Uniunea Europeană (retragere)], care încorporează legislația UE direct aplicabilă în dreptul Regatului Unit. În temeiul legii menționate, miniștrii Regatului Unit au competența de a introduce legislație secundară, prin intermediul instrumentelor statutare, pentru a aduce modificările necesare dreptului Uniunii menținut în dreptul intern în urma retragerii Regatului Unit din UE, astfel încât această legislație să corespundă contextului național.

14. În consecință, cadrul juridic relevant aplicabil în Regatul Unit după încheierea perioadei de tranziție[7] constă în:

- Regulamentul general privind protecția datelor al Regatului Unit (denumit în continuare „RGPD al Regatului Unit"), astfel cum a fost încorporat în dreptul Regatului Unit în temeiul Legii din 2018 privind Uniunea Europeană (retragere) și modificat prin Regulamentele DPPEC din 2019 [Protecția datelor, a vieții private și a comunicațiilor electronice (modificare etc.) (ieșirea din UE)];

[7] Perioada de tranziție se finalizează la 31 decembrie 2020, dată după care dreptul UE nu se mai aplică în Regatul Unit. „Perioada de grație" (perioada „bridge") se finalizează la 30 iunie 2021 cel târziu și se referă la perioada suplimentară în care transmiterea datelor cu caracter personal din UE către Regatul Unit nu este considerată transfer.

- DPA 2018, astfel cum a fost modificat prin Regulamentele DPPEC din 2019 și Regulamentele DPPEC din 2020 privind protecția datelor, a vieții private și a comunicațiilor electronice (modificări etc.) (ieșirea din UE); și
- Legea privind competența de investigare din 2016 (denumită în continuare „IPA 2016").

(denumite împreună „cadrul de protecție a datelor din Regatul Unit").

2.2 Domeniul de aplicare al evaluării CEPD

15. Proiectul de decizie al Comisiei Europene este rezultatul unei evaluări a cadrului de protecție a datelor din Regatul Unit, urmat de discuții purtate cu Guvernul Regatului Unit. În conformitate cu articolul 51 alineatul (1) litera (g) din LED, se așteaptă ca CEPD să prezinte un aviz independent cu privire la constatările Comisiei Europene, să identifice deficiențele cadrului de adecvare, dacă este cazul, și să depună eforturi de formulare a unor propuneri pentru abordarea acestora.

16. Astfel cum se menționează în criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul LED, „*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*"[8].

17. În acest sens, trebuie remarcat faptul că CEPD a primit numai o parte dintre documentele relevante pentru examinarea la timp a cadrului juridic din Regatul Unit. CEPD a primit cea mai mare parte a legislației Regatului Unit menționată în proiectul de decizie sub formă de link-uri inserate în acesta din urmă. Comisia Europeană nu a fost în măsură să furnizeze CEPD explicații și angajamente scrise din partea Regatului Unit în ceea ce privește schimburile de date care prezintă relevanță pentru acest exercițiu, realizate între autoritățile Regatului Unit și Comisia Europeană[9].

18. Ținând seama de cele de mai sus și având în vedere intervalul de timp limitat (2 luni) în care CEPD trebuie să adopte acest aviz, CEPD a ales să se concentreze asupra unor puncte specifice prezentate în proiectul de decizie și să își prezinte analiza și avizul asupra acestora. Întrucât procesul de analiză a vizat legislația și practicile unei țări terțe care a fost până de curând stat membru al UE, este evident că CEPD a identificat multe aspecte ca fiind în esență echivalente. Având în vedere rolul care îi revine în procesul de adoptare a unei constatări cu privire la caracterul adecvat al nivelului de protecție,

[8] A se vedea 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 aplicare a legii, punctul 15, p. 5.

[9] Acestea sunt elementele în cazul cărora Comisia Europeană se referă, în proiectul său de decizie, la explicații primite din partea autorităților Regatului Unit în condițiile nefurnizării de documente scrise din partea autorităților din Regatul Unit prin care să fie fundamentate explicațiile respective, cum ar fi cele referitoare la: efectele dispozițiilor tranzitorii și lipsa unei dispoziții de tip „sunset" privind încetarea de drept a efectelor juridice (considerentul 87); exemple de consimțământ ca bază adecvată pentru prelucrarea datelor (nota de subsol 68); noțiunea de date cu caracter personal „inexacte" cu înțelesul de „incorecte sau înșelătoare" (nota de subsol 79); domeniul de competența al Comisiei pentru Informații și Securitate a Parlamentului (*Intelligence and Security Committee* – ISC) (nota de subsol 245); pragul scăzut stabilit pentru depunerea unei plângeri la Tribunalul pentru competențe de investigare (*Investigatory Powers Tribunal* – IPT) și faptul că nu este neobișnuit ca IPT să stabilească faptul că, de fapt, persoana care a depus plângerea nu a făcut niciodată obiectul unei anchete din partea unei autorități publice (nota de subsol 263); combinația de competențe care decurge din legislație și dreptul comun (nota de subsol 52); prerogativele exercitate de guvern (nota de subsol 62); faptul că alte organizații au libertatea de a urma principiile din Codul de practici al sistemului de gestionare a informațiilor poliției [MoPI] (nota de subsol 86).

precum și numărul de legi și practici care trebuie analizate, CEPD a decis să își concentreze atenția asupra acelor aspecte cu privire la care a considerat că se impune o analiză mai atentă.

19. CEPD a luat în considerare cadrul european de protecție a datelor în vigoare, inclusiv articolele 7, 8 și 47 din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „Carta UE"), și anume protejarea dreptului la viață privată și de familie, dreptul la protecția datelor cu caracter personal și dreptul la o cale de atac eficientă și la un proces echitabil, precum și articolul 8 din Convenția europeană a drepturilor omului (denumită în continuare „CEDO") care prevede protejarea dreptului la viață privată și de familie. În plus față de cele de mai sus, CEPD a luat în considerare cerințele LED, precum și jurisprudența relevantă.

20. Obiectivul acestui exercițiu este de a oferi Comisiei Europene un aviz pentru evaluarea caracterului adecvat al nivelului de protecție din Regatul Unit. Acest concept de „nivel adecvat de protecție", care era deja prevăzut în temeiul Directivei 95/46/CE, a fost dezvoltat în continuare de CJUE. Este important de reamintit standardul stabilit de CJUE în *cauza Schrems I*, și anume că, 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"[10]. Prin urmare, obiectivul nu este de a reflecta punctual legislația europeană, ci de a stabili cerințele esențiale și de bază ale legislației examinate. 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 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 aplicare sunt de o importanță fundamentală pentru eficacitatea normelor de protecție a datelor[11].

2.3 Observații de natură generală și preocupări

2.3.1 Angajamente internaționale la care a aderat Regatul Unit

21. În conformitate cu articolul 36 alineatul (2) litera (c) din LED și cu criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul LED[12], atunci când evaluează caracterul adecvat al nivelului de protecție asigurat de o țară terță, Comisia Europeană ia în considerare, printre altele, angajamentele internaționale asumate de țara terță sau alte obligații care decurg din participarea țării terțe la sistemele multilaterale sau regionale, în special în ceea ce privește protecția datelor cu caracter personal, precum și punerea în aplicare a unor astfel de obligații. În plus, ar trebui să fie luată în considerare aderarea țării terțe la Convenția Consiliului Europei din 28 ianuarie 1981 pentru protejarea

[10] A se vedea cauza CJUE C-362/14, Maximilian Schrems împotriva Data Protection Commissioner, 6 octombrie 2015, ECLI:EU:C:2015:650 (denumită în continuare „cauza Schrems I"), punctele 73-74.
[11] A se vedea Recomandările CEPD 01/2021 cu privire la criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul Directivei privind protecția datelor în materie de aplicare a legii, punctul 14, p. 5.
[12] Recomandările CEPD 01/2021 cu privire la criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul Directivei privind protecția datelor în materie de aplicare a legii, punctul 24, p. 7.

persoanelor față de prelucrarea automatizată a datelor cu caracter personal (denumită în continuare „Convenția 108”)[13] și la protocolul adițional[14] la aceasta.

22. **În acest sens, CEPD salută faptul că Regatul Unit a aderat la CEDO și se află sub jurisdicția Curții Europene a Drepturilor Omului (denumită în continuare „CEDO”). În plus, Regatul Unit a aderat, de asemenea, la „Convenția 108” și la protocolul adițional la aceasta, a semnat „Convenția 108+”[15] în 2018 și lucrează în prezent la ratificarea acesteia.**

2.3.2 Posibila divergență viitoare a cadrului de protecție a datelor din Regatul Unit

23. Astfel cum se menționează în considerentul 171 din proiectul de decizie, Comisia Europeană trebuie să țină seama de faptul că, odată cu încheierea perioadei de tranziție prevăzute în Acordul de retragere[16], Regatul Unit administrează, aplică și asigură respectarea propriului regim de protecție a datelor și, de îndată ce dispoziția provizorie (dispoziția „bridge”)[17] prevăzută la articolul FINPROV.10A din Acordul comercial și de cooperare între UE și Regatul Unit[18] încetează să se aplice, acest lucru poate implica, în special, modificări ale cadrului de protecție a datelor evaluat în proiectul de decizie, precum și alte evoluții relevante.

24. Prin urmare, Comisia Europeană a decis să includă o clauză de încetarea de drept a efectelor juridice în proiectul său de decizie[19], stabilind data expirării la patru ani de la intrarea în vigoare a deciziei.

25. Este important de remarcat faptul că posibilitatea miniștrilor Regatului Unit și a secretarului de stat al Regatului Unit de a introduce legislație secundară după încheierea perioadei de grație poate conduce, în viitor, la o divergență semnificativă a cadrului de protecție a datelor din Regatul Unit față de cadrul de protecție a datelor din UE.

26. În cele din urmă, nu numai de la încheierea perioadei de tranziție, jurisprudența CJUE nu mai este obligatorie pentru Regatul Unit, ci, de asemenea, hotărârile deja adoptate ale CJUE, considerate jurisprudență reținută în cadrul juridic al Regatului Unit, ar putea să nu mai fie obligatorii pentru Regatul Unit, deoarece, în special, Regatul Unit are posibilitatea de a modifica dreptul Uniunii menținut

[13] A se vedea Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, „Convenția 108”, 28 ianuarie 1981.
[14] A se vedea Protocolul adițional la Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal în ceea ce privește autoritățile de supraveghere și fluxurile transfrontaliere de date, deschis spre semnare la 8 noiembrie 2001.
[15] A se vedea Protocolul de modificare a Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (denumit în continuare „Convenția 108+”), 18 mai 2018.
[16] A se vedea Acordul privind retragerea Regatului Unit al Marii Britanii și Irlandei de Nord din Uniunea Europeană și din Comunitatea Europeană a Energiei Atomice (JO L 029, 31.1.2020, p. 7).
[17] Perioada de tranziție se finalizează la 31 decembrie 2020, dată după care dreptul UE nu se mai aplică în Regatul Unit. „Perioada de grație” (perioada „bridge”) se finalizează la 30 iunie 2021 cel târziu și se referă la perioada suplimentară în care transmiterea datelor cu caracter personal din UE către Regatul Unit nu este considerată transfer.
[18] A se vedea Acordul comercial și de cooperare între Uniunea Europeană și Comunitatea Europeană a Energiei Atomice, pe de o parte, și Regatul Unit al Marii Britanii și Irlandei de Nord, pe de altă parte (JO L 444, 31.12.2020, p. 14).
[19] A se vedea articolul 4 din proiectul de decizie. A se vedea, de asemenea, considerentul 172 din proiectul de decizie.

în dreptul intern după încheierea perioadei de grație și Curtea Supremă a Regatului Unit nu se mai supune jurisprudenței UE reținute în jurisprudența internă[20].

27. **Având în vedere riscurile legate de posibila abatere a cadrului de protecție a datelor din Regatul Unit de la acquis-ul UE după încheierea perioadei de grație, CEPD salută decizia Comisiei Europene de a introduce în proiectul de decizie o clauză de încetare de drept a efectelor juridice cu un termen de patru ani. Cu toate acestea, CEPD ar dori să sublinieze în acest context importanța rolului de monitorizare al Comisiei Europene[21]. Într-adevăr, Comisia Europeană ar trebui să monitorizeze toate evoluțiile relevante din Regatul Unit care ar putea avea un impact asupra echivalenței în esență a nivelului de protecție a datelor cu caracter personal transferate în temeiul deciziei Regatului Unit privind caracterul adecvat al nivelului de protecție, în mod continuu și permanent, de la intrarea în vigoare a acestei decizii. În plus, Comisia Europeană ar trebui să ia măsuri corespunzătoare prin suspendarea, modificarea sau abrogarea deciziei privind caracterul adecvat al nivelului de protecție, în funcție de circumstanțele specifice, în cazul în care, după adoptarea deciziei privind caracterul adecvat al nivelului de protecție, Comisia Europeană are indicii că în Regatul Unit nu se mai asigură un nivel adecvat de protecție.**

28. La rândul său, CEPD va depune toate eforturile pentru a informa Comisia Europeană cu privire la orice acțiune relevantă întreprinsă de autoritățile de supraveghere a protecției datelor (denumite în continuare „AS") din statele membre, în special cu privire la plângerile formulate de persoanele vizate din UE în legătură cu transferul datelor cu caracter personal din UE către Regatul Unit.

3 NORME APLICABILE PENTRU PRELUCRAREA DATELOR CU CARACTER PERSONAL DE CĂTRE AUTORITĂȚILE COMPETENTE ÎN SCOPUL APLICĂRII LEGII

3.1 Domeniul de aplicare material

29. În ceea ce privește considerentul 24 și următoarele din proiectul de decizie, CEPD ia act de faptul că proiectul de decizie privind caracterul adecvat al nivelului de protecție nu conține multe detalii cu privire la activitățile și la cadrul juridic aplicabile altor agenții cu atribuții de aplicare a legii, în afară de poliție.

30. De exemplu, în cadrul explicativ al Regatului Unit pentru dezbateri privind caracterul adecvat al nivelului de protecție, secțiunea F: Aplicarea legii[22], se sugerează, la pagina 11, că **Agenția Națională de Combatere a Criminalității** (denumită în continuare „NCA") ar putea fi o autoritate de aplicare a legii de interes deosebit, care, printre altele, are o funcție mai vastă în ceea ce privește datele operative în materie penală. Conform propriei descrieri, NCA are misiunea de a centraliza date operative dintr-o serie de surse cu scopul de a maximiza oportunitățile de analiză, de evaluare și cu caracter tactic, provenite inclusiv din interceptarea cu mijloace tehnice a comunicațiilor, de la parteneri în domeniul

[20] A se vedea articolul 6 alineatele (3)-(6) din „European Union (Withdrawal) Act 2018" [Legea privind Uniunea Europeană din anul 2018 (retragere)].
[21] A se vedea articolul 36 alineatul (4) din LED.
[22] A se vedea cadrul explicativ al Regatului Unit pentru dezbateri privind caracterul adecvat al nivelului de protecție, secțiunea F: Asigurarea respectării legii, 13 martie 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

aplicării legii din Regatul Unit și din străinătate, de la agenții de securitate și de la agenții de informații[23]. NCA este, de asemenea, unul dintre principalii interlocutori pentru partenerii internaționali din domeniul aplicării legii și joacă un rol esențial în schimbul de date operative în materie penală[24].

31. CEPD observă că, de asemenea, Comandamentul de comunicații al guvernului (denumit în continuare „GCHQ"), ale cărui activități intră de obicei sub incidența părții 4 din DPA 2018, și anume securitatea națională, își asumă, de asemenea, un rol activ în reducerea prejudiciilor societale și financiare cauzate Regatului Unit de infracțiunile grave și de criminalitatea organizată, colaborând îndeaproape cu Ministerul de Interne, NCA, Administrația Fiscală și Vamală („HMRC") și alte departamente guvernamentale[25]. Activitățile comandamentului vizează combaterea abuzului sexual asupra minorilor, a fraudei, a altor tipuri de infracțiuni economice, inclusiv spălarea banilor, utilizarea tehnologiei pentru săvârșirea de infracțiuni, criminalitatea cibernetică, criminalitatea organizată în domeniul imigrației, inclusiv traficul de persoane, de droguri și de arme de foc și alte activități de contrabandă.

32. **CEPD solicită Comisiei Europene să își completeze analiza cu o examinare a autorităților care își desfășoară activitatea în domeniul aplicării legii și care par să fi făcut din colectarea și analizarea datelor, inclusiv a datelor cu caracter personal, un punct central al operațiunilor lor de zi cu zi, în special în cazul NCA. În plus, CEPD invită Comisia să analizeze cu mai mare atenție agențiile precum GCHQ, ale căror activități intră atât sub incidența aplicării legii și a securității naționale, cât și a cadrului juridic aplicabil acestora pentru prelucrarea datelor cu caracter personal.**

3.2 Garanții, drepturi și obligații

3.2.1 Prelucrarea datelor pe baza „consimțământului" persoanei vizate

33. CEPD ia act de faptul că, în considerentele 37 și 38 din proiectul de decizie, Comisia Europeană susține că **obținerea consimțământului** nu este considerată relevantă într-un scenariu care vizează caracterul adecvat al nivelului de protecție, deoarece, în situațiile de transfer, datele nu sunt colectate direct de la o persoană vizată de către o autoritate de aplicare a legii din Regatul Unit pe bază de consimțământ.

[23] A se vedea site-ul Agenției Naționale de Combatere a Criminalității, Date operative: evidențierea imaginii formelor grave de criminalitate organizată care afectează Regatul Unit, https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk.

[24] Deși nu toate datele operative prelucrate de NCA sunt date cu caracter personal, o parte substanțială ar putea consta în informații cu caracter personal, iar activitățile descrise în acest sens diferă de cele ale activităților polițienești clasice, astfel încât o evaluare a accesului la date cu caracter personal de către autoritățile de aplicare a legii din Regatul Unit ar fi incompletă fără o evaluare temeinică a activităților derulate de NCA. Pare rezonabil să se asigure faptul că principiile în materie de protecție a datelor au aceeași semnificație pentru toate autoritățile de aplicare a legii, oferind astfel clarificări în ceea ce privește o agenție care se bazează în mod special pe date, așa cum este NCA. În plus, la secțiunea „privind spre viitor", explicația continuă astfel: „căutăm în permanență noi oportunități de a atrage, dezvolta și consolida capabilitățile tradiționale pentru a spori cantitatea și calitatea datelor operative disponibile care pot fi exploatate atât în Regatul Unit cât și în străinătate". „În acest demers, dezvoltăm noua capabilitate națională de exploatare a datelor, utilizând competențele conferite agenției prin Legea privind criminalitatea și instanțele, pentru a corela, accesa și exploata datele deținute la nivel guvernamental." [...] „Toate acestea ne vor spori agilitatea și flexibilitatea în reacția la noi amenințări și ne vor permite să acționăm în mod proactiv, să colectăm și să analizăm informații și date operative cu privire la amenințările emergente astfel încât să putem acționa înainte ca amenințările să devină realitate."

[25] A se vedea site-ul GCHQ, Misiune, Infracțiuni grave și criminalitate organizată, https://www.gchq.gov.uk/section/mission/serious-crime.

34. În acest sens, CEPD reamintește că articolul 36 alineatul (2) litera (a) din LED impune evaluarea unei game largi de elemente care nu se limitează la situația transferului, inclusiv „statul de drept, respectarea drepturilor omului și a libertăților fundamentale, legislația relevantă, atât generală, cât și sectorială, inclusiv [...] dreptul penal”.

35. Consimțământul în contextul aplicării legii poate fi relevant ca temei juridic pentru prelucrarea datelor, ca o garanție suplimentară sau, în sens mai general, ca bază pentru exercitarea competențelor de investigare care conduc la obținerea datelor cu caracter personal, de exemplu, consimțământul unei părți terțe de a-i fi percheziționat sediul sau de a-i fi confiscate suporturile de stocare a datelor.

36. CEPD observă, inclusiv pe baza informațiilor furnizate de Comisia Europeană în considerentul 38 din proiectul de decizie, că utilizarea consimțământului, astfel cum este încadrat în regimul aplicabil în Regatul Unit, ar necesita întotdeauna invocarea unui temei juridic. Acest lucru înseamnă că, în pofida faptului că autoritatea polițienească are competențe statutare de a prelucra datele în scopul unei anchete, în anumite circumstanțe specifice (de exemplu, pentru prelevarea unei probe ADN), poliția poate considera oportun să solicite consimțământul persoanei vizate.

37. **CEPD invită Comisia Europeană să analizeze, în general, posibilitatea utilizării consimțământului într-un context de aplicare a legii atunci când evaluează caracterul adecvat al nivelului de protecție asigurat de o țară terță în temeiul LED.**

3.2.2 Drepturile omului

3.2.2.1 Certificate de securitate națională

38. În conformitate cu secțiunea 79 din DPA 2018, operatorii pot solicita certificate de securitate națională eliberate de un ministru, de un membru al guvernului, de procurorul general sau de avocatul general în cazul Scoției, care să ateste că limitele obligațiilor și drepturilor consacrate în capitolele 3 și 4 din partea 3 a DPA 2018 reprezintă o măsură necesară și proporțională pentru protecția securității naționale.

39. Aceste certificate sunt menite să confere operatorilor o mai mare securitate juridică și vor constitui dovezi concludente ale faptului că prelucrarea datelor cu caracter personal face obiectul securității naționale. Cu toate acestea, ar trebui menționat faptul că aceste certificate nu sunt obligatorii în sensul invocării unor restricții de securitate națională, ci reprezintă, mai degrabă, o măsură de transparență[26].

40. CEPD înțelege din secțiunile 17 și 18 din anexa 20 la DPA 2018, că un certificat de securitate națională eliberat în temeiul Legii privind protecția datelor din 1998 (denumit în continuare „vechiul certificat”) a avut un efect prelungit pentru prelucrarea datelor cu caracter personal în temeiul DPA 2018, până la 25 mai 2019. Până la această dată, cu excepția cazului în care au fost înlocuite sau revocate, vechile certificate au fost tratate ca și cum ar fi fost eliberate în temeiul DPA 2018. Cu toate acestea, în cazul în care un certificat de securitate națională eliberat în temeiul Legii privind protecția datelor din 1998 nu are o dată de expirare explicită, CEPD înțelege că un astfel de certificat va continua să producă efecte în ceea ce privește prelucrarea datelor în temeiul Legii privind protecția datelor din 1998, cu

[26] A se vedea Ministerul de Interne al Regatului Unit, Legea privind protecția datelor din 2018, Orientări cu privire la certificatele de securitate națională, august 2020 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf, p. 4.

excepția cazului în care respectivul certificat este revocat sau anulat[27]. Deși protecția asigurată de aceste vechi certificate se limitează la prelucrarea datelor cu caracter personal în temeiul Legii privind protecția datelor din 1998, CEPD constată că se pot emite noi certificate de securitate națională în temeiul Legii privind protecția datelor din 1998 pentru datele cu caracter personal care au fost prelucrate în temeiul Legii privind protecția datelor din 1998[28].

41. **Pentru asigurarea unui caracter cuprinzător, CEPD invită Comisia Europeană să clarifice în proiectul său de decizie cu privire la caracterul adecvat al nivelului de protecție faptul că certificatele de securitate națională se pot elibera în continuare în temeiul Legii privind protecția datelor din 1998. În plus, CEPD invită Comisia Europeană să descrie în proiectul său de decizie privind caracterul adecvat al nivelului de protecție mecanismele de reparații și de supraveghere în ceea ce privește certificatele eliberate în temeiul Legii privind protecția datelor din 1998. În cele din urmă, CEPD invită Comisia Europeană să includă în proiectul său de decizie privind caracterul adecvat al nivelului de protecție numărul de certificate existente eliberate în temeiul Legii privind protecția datelor din 1998 și să monitorizeze cu atenție acest aspect.**

3.2.2.2 Procesul decizional automatizat în temeiul LED

42. CEPD subliniază că articolul 11 alineatul (3) din LED interzice crearea de profiluri care are drept rezultat discriminarea persoanelor fizice pe baza categoriilor speciale de date cu caracter personal. Cu toate acestea, CEPD constată că articolul 50 din DPA 2018, care stabilește normele specifice pentru procesul decizional automatizat, nu prevede nicio astfel de interdicție.

43. **Prin urmare, CEPD invită Comisia Europeană să verifice acest aspect și să-și prezinte în mod explicit constatările în decizia sa privind caracterul adecvat al nivelului de protecție. În plus, CEPD invită Comisia Europeană să monitorizeze îndeaproape cazurile care se referă la procesul decizional automatizat și la crearea de profiluri.**

44. În conformitate cu criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul LED „dreptul 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”[29].

45. **CEPD invită Comisia să evalueze acest element în lumina orientărilor oferite de CEPD în criteriile sale de referință.**

3.2.3 Transferurile ulterioare

46. În conformitate cu criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul LED, 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. CEPD consideră că, astfel cum a fost subliniat de Comisia Europeană în

[27] A se vedea Ministerul de Interne al Regatului Unit, Legea privind protecția datelor din 2018, Orientări cu privire la certificatele de securitate națională, august 2020, p. 5.
[28] A se vedea Ministerul de Interne al Regatului Unit, Legea privind protecția datelor din 2018, Orientări cu privire la certificatele de securitate națională, august 2020, p. 5.
[29] A se vedea 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 aplicare a legii, punctele 59-61.

evaluarea sa, dispozițiile din partea 3 capitolul 5 din DPA 2018, în special secțiunea 73, prevăd, în principiu, un nivel de protecție care este în esență echivalent cu cel garantat în temeiul dreptului UE în ceea ce privește transferul datelor cu caracter personal de la o autoritate de aplicare a legii a Regatului Unit către o țară terță.

47. În primul rând, articolul 73 alineatul (1) litera (b) din DPA 2018 prevede în special că un operator de date nu poate transfera date cu caracter personal către o țară terță sau către o organizație internațională decât „în cazul în care datele cu caracter personal au fost inițial transmise sau puse în alt mod la dispoziția operatorului de date sau a unei alte autorități competente de către un stat membru altul decât Regatul Unit, statul membru respectiv sau orice persoană cu sediul în statul membru respectiv, care este o autoritate competentă în sensul Directivei privind protecția datelor în materie de aplicare a legii, a autorizat transferul în conformitate cu dreptul statului membru respectiv." Aceste dispoziții par a fi conforme cu criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul LED, care prevăd că trebuie avută în vedere, de asemenea, existența unui mecanism prin care autoritățile competente din statul membru în cauză 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 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. „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"[30].

48. **CEPD invită Comisia să evalueze acest element în lumina orientărilor oferite de CEPD în criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul LED.**

49. În al doilea rând, astfel cum s-a explicat în considerentul 81 al proiectului de decizie, secretarul de stat al Regatului Unit are competența de a recunoaște o țară terță (sau un teritoriu sau un sector dintr-o țară terță), o organizație internațională sau o descriere a țării, teritoriului, sectorului sau organizației respective, ca asigurând un nivel adecvat de protecție a datelor cu caracter personal, în urma consultării ICO[31]. Atunci când evaluează caracterul adecvat al nivelului de protecție, secretarul de stat al Regatului Unit trebuie să ia în considerare aceleași elemente pe care Comisia Europeană trebuie să le evalueze în temeiul articolului 36 alineatul (2) literele (a)-(c) din LED, interpretat în coroborare cu considerentul 67 din LED și cu jurisprudența UE reținută în jurisprudența internă. Aceasta înseamnă că, atunci când se evaluează nivelul adecvat de protecție al unei țări terțe, standardul relevant va fi dacă țara terță în cauză asigură un nivel de protecție „în esență echivalent" cu cel garantat în Regatul Unit. Deși CEPD ia act de capacitatea Regatului Unit, în temeiul DPA 2018, de a recunoaște teritoriile ca oferind un nivel de protecție adecvat în lumina cadrului de protecție a datelor din Regatul Unit, CEPD dorește să sublinieze că ar putea fi posibil ca aceste teritorii să nu beneficieze, până în prezent, de o decizie privind caracterul adecvat al nivelului de protecție, adoptată de Comisia Europeană prin care se recunoaște un nivel de protecție „în esență echivalent" cu cel garantat în UE. Acest lucru ar putea conduce la posibile riscuri în ceea ce privește protecția oferită datelor cu caracter personal transferate din UE, în special în cazul în care, în viitor, cadrul de protecție a datelor din Regatul Unit s-

[30] A se vedea 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 aplicare a legii, punctele 55 și 56.

[31] A se vedea articolul 182 alineatul (2) din DPA 2018. A se vedea, de asemenea, memorandumul de înțelegere privind rolul ICO în legătură cu noile evaluări cu privire la caracterul adecvat al nivelului de protecție asigurat în Regatul Unit, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/.

ar abate de la acquis-ul UE. Trebuie remarcat faptul că, în iulie 2020, cauza de referință *Schrems II* a CJUE[32] s-a soluționat cu declararea ca nevalidă a Deciziei SUA cu privire la scutul de confidențialitate, deoarece, potrivit CJUE, cadrul juridic al SUA nu a putut fi considerat ca oferind un nivel de protecție în esență echivalent cu cel al UE. Cu toate acestea, hotărârile CJUE deja adoptate, considerate ca fiind jurisprudență reținută în cadrul juridic al Regatului Unit, ar putea să nu mai fie obligatorii pentru Regatul Unit întrucât, în special, Regatul Unit are posibilitatea de a modifica dreptul Uniunii menținut în dreptul intern după încheierea perioadei de grație, iar Curtea Supremă nu are obligația de a se supune jurisprudenței UE reținute în jurisprudența internă[33].

50. **Prin urmare, CEPD invită Comisia Europeană să monitorizeze îndeaproape procesul și criteriile de evaluare a caracterului adecvat al nivelului de protecție utilizate de autoritățile din Regatul Unit cu privire la alte țări terțe, în special în ceea ce privește țările terțe pe care UE nu le recunoaște ca asigurând un nivel de protecție adecvat în temeiul LED.**

51. În cazul în care Comisia Europeană ar constata că o țară terță cu privire la care Regatul Unit consideră că asigură un nivel adecvat de protecție, nu oferă un nivel în esență echivalent cu cel garantat în UE, în conformitate cu articolul 36 din LED, **CEPD invită Comisia Europeană să ia toate măsurile necesare, cum ar fi, de exemplu, modificarea deciziei Regatului Unit privind caracterul adecvat al nivelului de protecție, pentru a introduce garanții specifice privind datele cu caracter personal care provin din UE și/sau pentru a lua în considerare suspendarea deciziei Regatului Unit privind caracterul adecvat al nivelului de protecție, în cazul în care datele cu caracter personal transferate din UE către Regatul Unit fac obiectul unor transferuri ulterioare către țara terță în cauză în baza regulamentului Regatului Unit cu privire la caracterul adecvat al nivelului de protecție**.

52. **În cele din urmă, în ceea ce privește acordurile internaționale încheiate sau care urmează să fie încheiate în viitor de Regatul Unit și posibilul acces al autorităților dintr-o țară terță (din țări terțe) care este/sunt parte la aceste acorduri, la datele cu caracter personal provenite din UE, CEPD recomandă Comisiei Europene să examineze corelarea dintre cadrul de protecție a datelor din Regatul Unit și angajamentele internaționale asumate de Regatul Unit, în special pentru a asigura continuitatea nivelului de protecție în cazul transferurilor ulterioare către alte țări terțe de date cu caracter personal transferate din UE către Regatul Unit în baza unei decizii a Regatului Unit privind caracterul adecvat al nivelului de protecție, precum și să monitorizeze în permanență și să ia măsuri, dacă este necesar, cu privire la încheierea de acorduri internaționale între Regatul Unit și țări terțe care prezintă riscul de a diminua nivelul de protecție a datelor cu caracter personal asigurat în UE**. De exemplu, deși Comisia Europeană a făcut referire la faptul că Acordul CLOUD dintre Regatul Unit și SUA[34] poate afecta transferurile ulterioare de date către SUA dinspre prestatorii de servicii din Regatul Unit, **CEPD subliniază că intrarea în vigoare a acestui acord poate afecta, de asemenea, transferurile ulterioare de date dinspre autoritățile de aplicare a legii ale Regatului Unit, în special în legătură cu emiterea și transmiterea de ordine în conformitate cu articolul 5 din Acordul CLOUD dintre Regatul Unit și SUA.**

53. CEPD consideră, de asemenea, că încheierea unor viitoare acorduri cu țări terțe în scopul cooperării în materie de aplicare a legii, prin care se asigură un temei juridic pentru transferul datelor cu caracter

[32] A se vedea cauza CJUE, C-311/18, Data Protection Commissioner împotriva Facebook Ireland Ltd și Maximilian Schrems, 16 iulie 2020, ECLI:EU:C:2020:559 (denumită în continuare „Schrems II").
[33] A se vedea articolul 6 alineatele (3)-(6) din „European Union (Withdrawal) Act 2018" [Legea privind Uniunea Europeană din anul 2018 (retragere)].
[34] A se vedea Acordul între Guvernul Regatului Unit al Marii Britanii și Irlandei de Nord și Guvernul Statelor Unite ale Americii privind accesul la datele electronice în scopul combaterii formelor grave de criminalitate, Washington DC, SUA, 3 octombrie 2019, https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.

personal către țările respective, poate afecta, de asemenea, în mod semnificativ, condițiile pentru schimbul ulterior de informații colectate, întrucât astfel de acorduri pot afecta cadrul juridic privind protecția datelor aplicat în Regatul Unit, astfel cum a fost acesta evaluat.

54. **Prin urmare, CEPD recomandă Comisiei Europene să monitorizeze în permanență dacă încheierea unor viitoare acorduri între Regatul Unit și țări terțe poate afecta aplicarea legislației Regatului Unit privind protecția datelor și să prevadă limitări sau excepțări suplimentare în ceea ce privește partajarea și utilizarea ulterioară a datelor, precum și divulgarea în străinătate a informațiilor colectate în scopul aplicării legii. CEPD consideră că astfel de informații și de evaluări sunt esențiale pentru a permite o revizuire cuprinzătoare a nivelului de protecție oferit de cadrul legislativ și de practicile utilizate în Regatul Unit cu privire la divulgarea datelor la nivel transfrontalier.**

55. În cele din urmă, CEPD ia act de faptul că, în conformitate cu secțiunea 76 alineatul (4) litera (b) din DPA 2018 (Transferuri în baza unor circumstanțe speciale), autoritățile de aplicare a legii din Regatul Unit pot transfera date cu caracter personal către o țară terță sau către o organizație internațională atunci când transferul „este necesar în scopul obținerii de consultanță juridică în legătură cu oricare dintre scopurile în materie de aplicare a legii". **CEPD subliniază că 38 din LED nu conține o dispoziție corespondentă, prin urmare, CEPD invită Comisia Europeană să clarifice ce se înțelege prin consultanță juridică și ce tip de date cu caracter personal sunt partajate în astfel de cazuri.**

3.2.4 Prelucrarea ulterioară, inclusiv schimbul ulterior de date pentru a garanta securitatea națională

56. În criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul LED, CEPD subliniase că, în ceea ce privește prelucrarea sau divulgarea ulterioară a datelor transferate din UE în alte scopuri decât cele de aplicare a legii, cum ar fi scopurile legate de securitatea națională, această prelucrare ar trebui, de asemenea, să fie prevăzută de lege, să fie necesară și proporțională. Astfel cum a fost evaluat de Comisia Europeană în proiectul său de decizie, articolul 36 alineatul (3) din DPA 2018, Legea privind economia digitală din 2017, Legea privind criminalitatea și instanțele din 2013 și Legea privind formele grave de criminalitate din 2017 prevăd un cadru juridic clar care permite partajarea ulterioară a datelor, stabilind că o astfel de partajare ulterioară trebuie să respecte normele prevăzute în DPA 2018.

57. CEPD observă că, în contextul prelucrării ulterioare, în alte scopuri, a datelor cu caracter personal transferate din UE, Comisia Europeană nu a evaluat dacă există mecanisme prin care autoritățile de aplicare a legii din Regatul Unit să informeze autoritățile competente relevante ale statele membre cu privire la o posibilă prelucrare ulterioară a datelor. Cu toate acestea, conform criteriilor de referință privind caracterul adecvat al nivelului de protecție în temeiul LED, se consideră că acesta este un element care trebuie luat în considerare[35]. În plus, existența unui astfel de mecanism de informare a autorităților competente relevante ale statelor membre cu privire la prelucrarea ulterioară a datelor cu caracter personal în scopul aplicării legii este considerată, de asemenea, un element care trebuie luat în considerare în cadrul criteriilor de referință privind caracterul adecvat al nivelului de protecție în temeiul LED[36].

58. **Prin urmare, CEPD invită Comisia Europeană să își completeze analiza cu informații referitoare la existența unor mecanisme prin care autoritățile de aplicare a legii ale Regatul Unit să notifice**

[35] A se vedea Recomandările 01/2021 ale CEPD cu privire la criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul Directivei privind protecția datelor în materie de aplicare a legii, punctul 41 și nota de subsol 39.

[36] A se vedea Recomandările 01/2021 ale CEPD cu privire la criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul Directivei privind protecția datelor în materie de aplicare a legii, alineatul 40.

autoritățile competente relevante din statele membre cu privire la o posibilă prelucrare ulterioară a datelor transferate din UE.

59. În plus, în ceea ce privește partajarea datelor colectate de o autoritate de aplicare a legii în materie penală, cu o agenție de informații, în scopul securității naționale, temeiul juridic care autorizează o astfel de partajarea ulterioară a datelor este legea privind combaterea terorismului din 2008. În acest sens, CEPD constată că domeniul de aplicare și dispozițiile articolului 19 din Legea privind combaterea terorismului din 2008 nu sunt abordate pe deplin în evaluarea Comisiei Europene și pot implica o utilizare ulterioară cu un caracter mai amplu, în special în ceea ce privește articolul 19 alineatul (2) din Legea privind combaterea terorismului din 2008, care prevede că „informațiile obținute de oricare dintre serviciile de informații în legătură cu exercitarea oricăreia dintre funcțiile care îi revin pot fi utilizate de serviciul în cauză pentru exercitarea oricărei alte funcții din domeniul său de competență". În acest caz, CEPD subliniază că, atunci când sunt prelucrate sau divulgate ulterior, datele ar trebui să beneficieze de același nivel de protecție ca atunci când au fost prelucrate inițial de autoritatea competentă destinatară.

3.3 Supraveghere și aplicare

60. CEPD observă că supravegherea autorităților de aplicare a legii în materie penală este asigurată de o combinație de diferiți comisari, pe lângă ICO. În constatările din proiectul de decizie privind caracterul adecvat al nivelului de protecție sunt menționați comisarul cu competențe de investigare (denumit în continuare „IPC"), comisarul pentru reținerea și utilizarea materialelor biometrice, precum și comisarul pentru camere de supraveghere. În acest context, trebuie remarcat faptul că CJUE a subliniat în repetate rânduri necesitatea unei supravegheri independente. O importanță deosebită în ceea ce privește accesul la date cu caracter personal transferate către Regatul Unit revine activităților realizate de comisarul cu competențe de investigare (IPC). În înțelegerea CEPD, IPC este așa-numitul „comisar judiciar", la fel ca alți comisari judiciari, la care se face referire în contextul capitolului dedicat securității naționale, iar acești comisari judiciari se bucură de independența conferită judecătorilor inclusiv atunci când exercită funcția de comisari. În ceea ce privește biroul IPC, Comisia Europeană explică, în considerentul 245 al proiectului de decizie, că acesta funcționează independent, sub forma unui așa-numit „organism ce funcționează în condiții obiective", deși este finanțat de Ministerul de Interne.

61. În plus, IPC îi revine, de asemenea, competența asupra controlului *ex post* al măsurilor de supraveghere. Cu toate acestea, se pare că, în această calitate, rolul IPC este acela de a formula recomandări în cazuri de nerespectare și de a informa persoana vizată în cazul în care eroarea este gravă și este în interesul public ca persoana să fie informată.

62. CEPD nu a identificat în proiectul de decizie indicații suplimentare pe baza cărora să poată evalua independența comisarului pentru reținerea și utilizarea materialelor biometrice și a comisarului pentru camere de supraveghere.

63. **Comisia Europeană este invitată să evalueze în continuare independența comisarilor judiciari, inclusiv în cazurile în care comisarul nu (mai) îndeplinește funcția de judecător, și să evalueze independența comisarului pentru reținerea și utilizarea materialelor biometrice și a comisarului pentru camere de supraveghere.**