Avizul 27/2025 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 de către

Regatul Unit al Marii Britanii și Irlandei de Nord

Adoptat la 16 octombrie 2025

Rezumat

La 22 iulie 2025, Comisia Europeană a aprobat proiectul său de decizie de punere în aplicare privind protecția adecvată a datelor cu caracter personal de către Regatul Unit în temeiul Directivei privind protecția datelor în materie de aplicare a legii. La aceeași dată, în cadrul procedurii de adoptare formală a proiectului de decizie, Comisia Europeană a solicitat avizul Comitetului European pentru Protecția Datelor.

Proiectul de decizie modifică și completează decizia anterioară privind caracterul adecvat al nivelului de protecție pentru Regatul Unit în temeiul Directivei privind protecția datelor în materie de aplicare a legii, care datează din iunie 2021. Evaluarea de către CEPD a caracterului adecvat al nivelului de protecție oferit de Regatul Unit a fost efectuată pe baza examinării proiectului de decizie și, prin urmare, se axează pe noile evoluții ale legislației Regatului Unit privind protecția datelor și pe elementele evidențiate în decizia anterioară privind caracterul adecvat al nivelului de protecție.

CEPD a utilizat criteriile sale de referință privind caracterul adecvat al nivelului de protecție în temeiul LED, adoptate la 2 februarie 2021, ca referință principală pentru această activitate, precum și Recomandările 02/2020 ale CEPD privind garanțiile esențiale europene pentru măsurile de supraveghere și jurisprudența relevantă. CEPD salută alinierea continuă dintre cadrul de protecție a datelor din Regatul Unit și cel al UE, în pofida evoluțiilor recente ale cadrului juridic relevant al Regatului Unit. În acest context, este important să se sublinieze că, potrivit așteptărilor CEPD, cadrul juridic al Regatului Unit nu va reproduce legislația europeană privind protecția datelor, obiectivul prezentului aviz fiind de a identifica aspecte specifice ale modificărilor și evoluțiilor juridice de la adoptarea primei decizii privind caracterul adecvat al nivelului de protecție, care pot afecta nivelul de protecție, și de a aduce în discuție preocupări sau aspecte care necesită clarificări suplimentare, atenție și monitorizare.

În acest sens, CEPD evidențiază în continuare o serie de constatări:

CEPD observă modificări ale normelor care reglementează transferul ulterior de date cu caracter personal către țări terțe, în special noua listă orientativă de elemente care trebuie luate în considerare în testul de evaluare a caracterului adecvat al nivelului de protecție, care nu include elemente importante care au figurat în testul anterior de evaluare a caracterului adecvat al nivelului de protecție din Regatul Unit. CEPD consideră că acest aspect, precum și noul criteriu de „oportunitate a facilitării transferurilor de date cu caracter personal către și dinspre Regatul Unit" trebuie abordate mai detaliat și încurajează Comisia Europeană să își detalieze în mod specific evaluarea și să monitorizeze evoluțiile și punerea în practică a noului test de evaluare a caracterului adecvat.

CEPD ia act de schimbările importante în ceea ce privește modul în care procesul decizional automatizat este reglementat în Regatul Unit, în special introducerea unei abordări mai permisive și conferirea de noi competențe secretarului de stat. Domeniul de aplicare și marja de apreciere a acestor competențe ar putea da naștere unor preocupări semnificative, de exemplu din cauza amplorii lor, în special având în vedere evoluția rapidă a mediului de reglementare și progresele înregistrate în domeniul tehnologiilor automatizate. CEPD invită Comisia Europeană să analizeze aceste competențe și să monitorizeze orice evoluție în acest sens. CEPD reamintește, de asemenea, importanța unei verificări umane semnificative pentru a asigura respectarea garanțiilor în procesul decizional automatizat și, prin urmare, îndeamnă Comisia Europeană să detalieze în continuare posibilele derogări de la dreptul persoanei vizate de a obține intervenție umană în decizia sa finală privind caracterul adecvat al nivelului de protecție și să monitorizeze punerea în aplicare a acestor modificări în practică.

CEPD consideră că este esențial să se evalueze derogările extinse în materie de securitate națională în temeiul cadrului de aplicare a legii și rămâne deosebit de vigilent în ceea ce privește orice derogare de la principiul proporționalității, precum și de la cerința de a prelucra datele cu caracter personal într-un scop legitim. De asemenea, orice derogări de la competențele autorității de supraveghere trebuie abordate cu prudență. Orice restrângere a exercițiului drepturilor și libertăților recunoscute de Carta drepturilor fundamentale a UE trebuie să respecte esența acestora și, sub rezerva principiului proporționalității, poate fi impusă numai în cazul în care este necesară și numai dacă răspunde efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți. CEPD invită Comisia Europeană să își completeze evaluarea în decizia finală privind caracterul adecvat al nivelului de protecție și să monitorizeze în mod specific aplicarea în practică a derogărilor în materie de securitate națională pentru autoritățile de aplicare a legii.

CEPD observă că activitățile de prelucrare desfășurate de autoritățile competente pentru asigurarea respectării legii pot intra, în anumite circumstanțe, sub incidența normelor aplicabile în mod normal prelucrării datelor cu caracter personal de către autoritățile naționale de securitate. În acest context, ar trebui să se acorde o atenție deosebită asigurării faptului că regimul de protecție a datelor pentru prelucrarea în scopul securității naționale nu este extins la contexte care nu au legătură cu securitatea națională. CEPD invită Comisia Europeană să monitorizeze în practică dacă autoritățile competente calificate sunt în măsură să mențină o distincție clară între diferitele scopuri ale prelucrării pentru a adera în consecință la cadrul juridic corespunzător.

Deși recunoaște că sistemul de supraveghere a agențiilor de aplicare a dreptului penal, precum și mecanismele de recurs rămân în mare măsură neschimbate, CEPD reiterează necesitatea monitorizării îndeaproape de către Comisia Europeană a aplicării competențelor corective și a căilor de atac pentru persoanele vizate în cadrul de protecție a datelor din Regatul Unit.

Pe lângă reintroducerea unei clauze de caducitate și a obligației legale de monitorizare, CEPD subliniază că este important ca Comisia Europeană să efectueze revizuirea obligatorie în termenul legal specificat în Directiva privind protecția datelor în materie de aplicare a legii, ținând seama de elementele deja prezentate în Decizia de punere în aplicare 2021/1773 a Comisiei, precum și de orice alte evoluții relevante.

Cuprins

1 INTRODUCERE 5

1.1 Observații generale 5

1.2 Domeniul de aplicare al prezentului aviz al CEPD 6

1.3 Evoluții relevante ale cadrului juridic din Regatul Unit 7

2 EVOLUȚII RELEVANTE ÎN CEEA CE PRIVEȘTE NORMELE APLICABILE PRELUCRĂRII DATELOR CU CARACTER PERSONAL 7

2.1 Garanții, drepturi și obligații 7

2.1.1 Utilizarea consimțământului în contextul aplicării legii 7

2.1.2 Transferuri ulterioare 8

2.1.3 Procesul decizional automatizat 9

2.1.4 Cerințe privind înregistrarea 11

2.1.5 Derogări din motive de securitate națională pentru autoritățile de aplicare a legii 11

2.1.6 Exercitarea în comun a competenței de operator între serviciile de informații din Regatul Unit și autoritățile de aplicare a legii 13

2.1.7 Dreptul de acces 14

2.1.8 Supravegherea și căile de atac 14

3 Revizuirea, durata și reînnoirea deciziei 16

Comitetul European pentru Protecția Datelor

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 (denumită în continuare „LED”),

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

ADOPTĂ PREZENTUL AVIZ:

1 INTRODUCERE

1.1 Observații generale

1. La 22 iulie 2025, Comisia Europeană (denumită în continuare „Comisia”) a aprobat proiectul său de decizie de punere în aplicare privind protecția adecvată a datelor cu caracter personal de către Regatul Unit în temeiul LED (denumit în continuare „proiectul de decizie”). La aceeași dată, în cadrul procedurii de adoptare formală a proiectului de decizie, Comisia Europeană a solicitat avizul Comitetului European pentru Protecția Datelor („CEPD”). CEPD ia act de faptul că proiectul de decizie prelungește valabilitatea deciziei existente privind caracterul adecvat al nivelului de protecție asigurat de Regatul Unit[1] cu o perioadă de șase ani, până la 27 decembrie 2031. CEPD amintește că decizia inițială privind caracterul adecvat al nivelului de protecție urma să expire la 27 iunie 2025 și, prin urmare, făcuse deja obiectul unei prelungiri tehnice și limitate în timp[2] pentru a permite Regatului Unit să își finalizeze reformele în materie de protecție a datelor[3]. Testul aplicat de Comisie acestei evaluări constă în a evalua „dacă este în continuare justificată, din punct de vedere factual și juridic, concluzia potrivit căreia Regatul Unit asigură un nivel adecvat de protecție, având în vedere evoluțiile care au avut loc de la adoptarea deciziei anterioare privind caracterul adecvat al nivelului de protecție în Regatul Unit”[4]. Prin urmare, Comisia și-a axat evaluarea pe noua legislație privind protecția datelor, Legea în materie de (utilizare și acces la) date („DUAA”), care a intrat în vigoare la 20 august 2025. Comisia a luat în considerare în mod specific elementele enumerate în considerentul 165 din decizia anterioară privind caracterul adecvat al nivelului de protecție din Regatul Unit, care figurează toate în proiectul de decizie, și anume:

[1] Decizia de punere în aplicare (UE) 2021/1773 a Comisiei din 28 iunie 2021 în temeiul Directivei (UE) 2016/680 a Parlamentului European și a Consiliului privind protecția adecvată a datelor cu caracter personal de către Regatul Unit al Marii Britanii și Irlandei de Nord [notificată cu numărul C(2021) 4801].

[2] Decizia de punere în aplicare (UE) 2025/1225 a Comisiei din 24 iunie 2025 de modificare a Deciziei de punere în aplicare (UE) 2021/1773 în temeiul Directivei (UE) 2016/680 a Parlamentului European și al Consiliului privind protecția adecvată a datelor cu caracter personal de către Regatul Unit [notificată cu numărul C(2025) 3898].

[3] Avizul 06/2025 privind prelungirea deciziilor de punere în aplicare ale Comisiei Europene adoptate în temeiul RGPD și al Directivei privind protecția datelor în materie de aplicare a legii (*Directive on Law Enforcement* - LED) cu privire la protecția adecvată a datelor cu caracter personal în Regatul Unit, adoptat la 5 mai 2025, disponibil la următorul link: https://www.edpb.europa.eu/system/files/2025-05/edpb-opinion-202506-uk-adequacyextension-gdpr-led_en.pdf.

[4] A se vedea considerentul 4 din proiectul de decizie.

„normele privind transferurile de date cu caracter personal către țări terțe și impactului pe care aceasta l-ar putea avea asupra nivelului de protecție acordat datelor transferate în temeiul prezentei decizii, precum și eficacității exercitării drepturilor individuale, inclusiv orice evoluție relevantă în legislație și în practică în ceea ce privește excepțiile sau restricțiile referitoare la astfel de drepturi. Printre alte elemente, evoluțiile jurisprudenței și supravegherea de către Biroul Comisarului pentru Informații (ICO) și de către alte organisme independente au stat la baza monitorizării din partea Comisiei." [5]

2. Comisia concluzionează că, pe baza acestei evaluări, Regatul Unit continuă să garanteze un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniunea Europeană către Regatul Unit în cadrul domeniului de aplicare al Directivei (UE) 2016/680.

3. CEPD este de acord că evaluarea ar trebui să se concentreze în principal pe noile evoluții ale legislației din Regatul Unit privind protecția datelor și pe elementele evidențiate în decizia anterioară privind caracterul adecvat al nivelului de protecție. În opinia CEPD, Comisia a evaluat toate elementele enumerate la articolul 36 alineatul (2) din LED și toate evoluțiile relevante ale cadrului juridic general al Regatului Unit dincolo de DUAA atunci când a ajuns la concluzia potrivit căreia cadrul juridic general al Regatului Unit continuă să garanteze un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniunea Europeană către Regatul Unit în cadrul domeniului de aplicare al LED. Cu toate acestea, CEPD ar aprecia o clarificare explicită în acest sens în decizia finală privind caracterul adecvat al nivelului de protecție. CEPD ar aprecia, de asemenea, o clarificare din partea Comisiei potrivit căreia va continua să evalueze aceste elemente în mod continuu, ca parte a rolului său de monitorizare.

4. Având în vedere că unele modificări legislative, cerințe juridice și garanții se aplică în mod similar atât în cadrul regimului de acces al administrației publice, cât și în cadrul LED, evaluările corespunzătoare efectuate de CEPD vor fi încorporate atât în prezentul aviz, cât și în Avizul 26/2025, pentru a asigura coerența și exhaustivitatea.

5. CEPD ia act, de asemenea, de faptul că, în temeiul articolelor 47 și 94 din Regulamentul (UE) 2018/1725[6], instituțiile, organele, oficiile și agențiile Uniunii Europene pot transfera date cu caracter personal către o țară terță, un teritoriu, un sector sau o organizație internațională recunoscută de Comisie în temeiul articolului 36 alineatul (3) din LED a asigurând un nivel adecvat de protecție, cu condiția ca transferul să îndeplinească exclusiv sarcini care țin de competența operatorului, fără a fi necesară o autorizație suplimentară. Având în vedere cooperarea existentă între agențiile de aplicare a legii ale Uniunii, cum ar fi Europol și Eurojust, și omologii lor din Regatul Unit, CEPD invită Comisia să reamintească această posibilitate juridică în considerentele proiectului de decizie.

1.2 Domeniul de aplicare al prezentului aviz al CEPD

6. În conformitate cu articolul 51 alineatul (1) litera (g) din LED, se preconizează că CEPD va prezenta Comisiei un aviz independent pentru evaluarea caracterului adecvat al nivelului de protecție într-o țară terță. Având în vedere situația specifică a Regatului Unit, proiectul de decizie completează decizia din 2021 privind caracterul adecvat al nivelului de protecție, care rămâne valabilă pentru părțile care nu sunt abordate în mod specific în proiectul de decizie. La fel ca în prezentul aviz, CEPD se bazează pe

[5] A se vedea considerentul 6 din proiectul de decizie.

[6] Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE („EUDPR"), JO L 295, 21.11.2018, p. 39.

avizul său anterior, pe care îl dezvoltă în continuare[7]. Prin urmare, analiza CEPD și observațiile furnizate în acesta continuă, în general, să se aplice.

7. Având în vedere cele de mai sus și din cauza termenului limitat acordat CEPD pentru adoptarea prezentului aviz, CEPD și-a concentrat observațiile și analiza asupra anumitor puncte prezentate în proiectul de decizie, în special atunci când sunt necesare clarificări suplimentare, informații suplimentare sau o monitorizare viitoare din partea Comisiei.

1.3 Evoluții relevante ale cadrului juridic din Regatul Unit

8. Astfel cum se explică în proiectul de decizie[8], după încheierea perioadei de punere în aplicare convenite în Acordul de retragere dintre Regatul Unit și UE[9] la 31 decembrie 2020, Regatul Unit intenționa să adopte un nou regim de protecție a datelor, care era diferit de cadrul juridic al UE. Între timp, Regatul Unit a adoptat modificări ale cadrului său existent de protecție a datelor, în principal prin intermediul DUAA, care prevede modificări limitate ale diferitelor aspecte ale cadrului.

9. Prezentul aviz abordează modificările legislative relevante introduse prin DUAA și modul în care aceste modificări afectează protecția datelor în cadrul Regatului Unit. Deși majoritatea modificărilor introduse în cadrul de protecție a datelor din Regatul Unit vizează clarificarea și facilitarea respectării legii, CEPD consideră că unele dintre noile modificări juridice netestate, care pot afecta nivelul de protecție, în funcție de punerea lor în aplicare, ar trebui să facă obiectul unor clarificări suplimentare și al monitorizării cu atenție din partea Comisiei. Din explicațiile suplimentare furnizate de Comisie, CEPD înțelege că aceasta intenționează să examineze evoluția unora dintre aceste modificări și invită Comisia să evidențieze în decizia finală domeniile pe care intenționează să le monitorizeze cu atenție.

2 EVOLUȚII RELEVANTE ÎN CEEA CE PRIVEȘTE NORMELE APLICABILE PRELUCRĂRII DATELOR CU CARACTER PERSONAL

2.1 Garanții, drepturi și obligații

2.1.1 Utilizarea consimțământului în contextul aplicării legii

10. CEPD ia act de explicațiile oferite de Comisie cu privire la modificările tehnice aduse definiției[10], condițiilor de obținere a consimțământului[11] și alinierii generale a conceptului de consimțământ din partea a doua și partea a treia din Legea privind protecția datelor din 2018 („DPA din 2018"), întrucât considerentele 35 și 36 din Decizia de punere în aplicare 2021/1773 rămân valabile – și anume,

[7] 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.
[8] A se vedea considerentul 2 din proiectul de decizie.
[9] Perioada de punere în aplicare este o perioadă convenită în Acordul de retragere dintre Regatul Unit și UE, în care Regatul Unit nu va mai fi membru al UE, dar va continua să se supună normelor UE și să rămână membru al pieței unice și al uniunii vamale. A se vedea Legea (Acordul de retragere) din Uniunea Europeană din 2020.
[10] A se vedea secțiunea 69 alineatul (2) punctul 1A din Legea în materie de (utilizare și acces la) date din 2025, care va introduce următoarea definiție a consimțământului: „o manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal să fie prelucrate", folosindu-se aceeași formulare ca la articolul 4 alineatul (11) din RGPD al Regatului Unit din 2018.
[11] A se vedea secțiunea 69 alineatul (4) din Legea în materie de (utilizare și acces la) date din 2025, care va defini condițiile privind acordarea consimțământului.

consimțământul nu constituie în sine un temei juridic pentru prelucrarea, inclusiv transferul, datelor cu caracter personal în contextul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor.

11. CEPD apreciază faptul că, la fel ca în evaluarea din 2021, Comisia a examinat utilizarea consimțământului în contextul asigurării respectării legii. CEPD reamintește faptul că „consimțământul persoanei vizate nu ar trebui să constituie un temei juridic pentru prelucrarea datelor cu caracter personal de către autoritățile competente”[12]. Prin urmare, CEPD reafirmă necesitatea de a efectua o astfel de analiză atunci când se evaluează nivelul de protecție în temeiul articolului 36 din LED[13].

2.1.2 Transferuri ulterioare

12. Atunci când o autoritate competentă intenționează să facă schimb de date cu caracter personal prelucrate în temeiul părții 3 din DPA din 2018 cu autoritățile de aplicare a legii dintr-o țară terță, se aplică anumite cerințe. În special, astfel de transferuri pot avea loc atunci când sunt aprobate prin regulamentele adoptate de secretarul de stat sau, în lipsa acestor regulamente, pe baza unor garanții adecvate. În cazul în care un transfer nu se poate baza nici pe un regulament, nici pe garanții adecvate, acesta poate avea loc numai în anumite circumstanțe specificate, denumite „circumstanțe speciale”, corespunzătoare situațiilor și condițiilor care se califică drept „derogări” în temeiul articolului 38 din LED.

13. Deși Comisia observă că „regimul privind transferurile internaționale de date cu caracter personal din Regatul Unit rămâne foarte apropiat de normele prevăzute în capitolul V din Directiva (UE) 2016/680”, proiectul de decizie indică, de asemenea, că standardul juridic pentru reglementările de aprobare a transferurilor, care erau denumite reglementări privind caracterul adecvat al nivelului de protecție în fosta secțiune 74A din DPA din 2018, și garanțiile adecvate au fost reformulate. În loc să se refere la un nivel adecvat de protecție, noul „criteriu privind protecția datelor” prevăzut în secțiunea 74AB din DPA din 2018 impune ca standardul de protecție pentru persoanele vizate din țările terțe sau din cadrul organizațiilor internaționale destinatare să nu fie „cu mult inferior” decât standardului prevăzut pentru persoanele vizate în temeiul legislației relevante a Regatului Unit privind protecția datelor.

14. În acest context, CEPD ia act de faptul că elementele care trebuie luate în considerare de secretarul de stat în evaluarea caracterului adecvat în conformitate cu secțiunea 74AB alineatul (2) din DPA din 2018 par să fi fost reduse în comparație cu evaluarea anterioară a reglementărilor privind caracterul adecvat al nivelului de protecție[14]. CEPD subliniază eliminarea anumitor factori care, în opinia sa, au un rol important în evaluarea măsurii în care o țară terță oferă un nivel de protecție a datelor cu caracter personal echivalent în esență. Printre acestea se numără, în special, (i) normele țării terțe în ceea ce privește „siguranța publică, apărarea, securitatea națională și dreptul penal și accesul autorităților publice la datele cu caracter personal”, (ii) jurisprudența, (iii) evaluarea globală a cadrului juridic relevant, inclusiv în ceea ce privește accesul autorităților publice la date, (iv) existența unor drepturi efective și opozabile ale persoanelor vizate (v) și trimiterea la una sau mai multe autorități de supraveghere independente funcționale (în schimb, noul criteriu se referă la o „autoritate responsabilă cu asigurarea respectării protecției persoanelor vizate în ceea ce privește prelucrarea datelor cu caracter personal”).

[12] Astfel cum a afirmat CEPD în considerentul 35 din 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.
[13] A se vedea considerentul 37 din Avizul CEPD 15/2021.
[14] Dispoziția eliminată acum din secțiunea 74A alineatul (4) din DPA din 2018 prevedea o listă de criterii care era identică cu articolul 36 alineatul (3) din LED.

15. Deși este recunoscut faptul că criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul LED oferă doar detalii limitate cu privire la acest aspect, CEPD reamintește declarația sa potrivit căreia „transferurile ulterioare de date cu caracter personal de către destinatarul inițial către o altă țară terță sau organizație internațională nu trebuie să submineze nivelul de protecție, prevăzut în Uniune, al persoanelor fizice ale căror date sunt transferate", care nu poate fi interpretată ca neincluzând necesitatea unei autorități de supraveghere independente și a unor drepturi efective și opozabile ale persoanelor vizate. Prin urmare, CEPD încurajează Comisia să abordeze în mod specific aceste modificări și să continue elaborarea evaluării noului criteriu privind protecția datelor.

16. CEPD înțelege că noile norme privind transferurile de date cu caracter personal către țări terțe sunt destinate să asigure o flexibilitate suplimentară. În același timp, CEPD invită Comisia să monitorizeze aplicarea practică a acestor norme. Acest lucru este deosebit de relevant în ceea ce privește noua competență a secretarului de stat de a elabora reglementări care să identifice și să aprobe un transfer, pe baza noului criteriu privind protecția datelor, prin orice mijloace, inclusiv prin referire la sectoarele geografice din interiorul unei țări, operatorii sau persoanele împuternicite de operatori, destinatarii datelor, tipurile de date, mijloacele de transfer și instrumentele juridice. Rămâne neclar, de exemplu, modul în care un anumit operator sau o anumită persoană împuternicită de operator cu sediul într-o țară terță care nu este considerată adecvată ar îndeplini criteriul privind protecția datelor în ceea ce privește căile de atac efective sau drepturile persoanelor vizate care nu sunt deja stabilite în cadrul juridic al țării terțe respective.

17. În plus, CEPD invită Comisia să clarifice în decizia sa faptul că criteriul „oportunității facilitării transferurilor de date cu caracter personal către și dinspre Regatul Unit" [secțiunea 74AA alineatul (3) din Legea privind protecția datelor din 2018] nu este un element al criteriului privind protecția datelor, ci doar un factor suplimentar pe care secretarul de stat îl poate lua în considerare în cazul în care criteriile testului sunt îndeplinite pe deplin, deoarece acest lucru nu reiese în mod clar din textul legii. În acest sens, CEPD invită Comisia să monitorizeze implicațiile practice ale secțiunii 74AA alineatul (3) din DPA din 2018, deoarece rămâne de văzut ce rol va îndeplini în acest context „oportunitatea facilitării transferurilor de date cu caracter personal către și dinspre Regatul Unit".

2.1.3 Procesul decizional automatizat

18. CEPD ia act de secțiunea 80 din DUAA, care introduce modificări importante ale modului în care procesul decizional automatizat este reglementat în Regatul Unit. CEPD observă că DUAA adoptă o abordare mai permisivă, ceea ce reprezintă o îndepărtare de la abordarea mai restrictivă a UE. În general, persoanele își pierd dreptul de a nu fi supuse unor decizii automatizate, cu excepția cazurilor care implică date sensibile. Prin noile secțiuni 50A-50D din DPA din 2018, autoritățile de aplicare a legii pot lua decizii semnificative utilizând procese automatizate, indiferent de temeiul juridic pe care se bazează, cu condiția să pună în aplicare garanții adecvate. Aceste garanții includ furnizarea de informații persoanei vizate cu privire la deciziile semnificative luate pe baza mijloacelor automatizate și la prelucrarea aferentă a datelor cu caracter personal, în mod similar cu articolul 11 și cu considerentul 38 din LED. În plus, persoanei vizate trebuie să i se ofere posibilitatea de a formula observații cu privire la astfel de decizii, de a obține intervenție umană din partea operatorului pentru a revizui decizia automatizată și de a contesta o astfel de decizie[15].

19. Prin urmare, accentul legii se schimbă de la restricționarea utilizării procesului decizional automatizat la asigurarea faptului că există transparență, verificare umană și controale ale riscurilor. Deși Comisia recunoaște această schimbare în considerentul 43 și o analizează în considerentul 47, CEPD invită

[15] Secțiunea 50C alineatul (2) din DPA din 2018.

Comisia să explice mai detaliat de ce consideră că noua abordare continuă să ofere un nivel suficient de protecție. În consecință, CEPD încurajează Comisia să includă o analiză mai detaliată a acestei schimbări substanțiale în decizia finală privind caracterul adecvat al nivelului de protecție.

20. CEPD ia act, de asemenea, de marja de apreciere acordată secretarului de stat în contextul procesului decizional automatizat[16]. CEPD înțelege că secretarului de stat i se acordă o marjă largă de apreciere în ceea ce privește stabilirea a ceea ce se califică drept „implicare umană semnificativă" și „decizie semnificativă care are un efect la fel de semnificativ". Domeniul de aplicare și marja de apreciere a acestor competențe ar putea da naștere unor preocupări semnificative, de exemplu din cauza amplorii lor, în special având în vedere evoluția rapidă a mediului de reglementare și progresele înregistrate în domeniul tehnologiilor automatizate, cum ar fi IA. Prin urmare, CEPD invită Comisia să analizeze aceste competențe nou-conferite secretarului de stat și să monitorizeze orice evoluții în acest sens.

21. În acest context, CEPD subliniază în mod specific rolul și relevanța dreptului persoanei vizate de a obține intervenție umană. Criteriile de referință ale CEPD privind caracterul adecvat al nivelului de protecție în temeiul LED subliniază importanța acestui drept, în special de a-și exprima punctul de vedere, de a primi o explicație privind decizia luată în urma unei astfel de evaluări sau de a contesta decizia[17]. Deși dreptul de a obține intervenție umană continuă, în general, să fie una dintre principalele garanții în cazul unui proces decizional automatizat, CEPD ia act de faptul că în cadrul de aplicare a legii din Regatul Unit a fost introdusă o nouă derogare care permite autorităților de aplicare a legii să nu aplice garanțiile enumerate în secțiunea 50C alineatul (2) din DPA din 2018, de exemplu pentru a evita obstrucționarea unei investigații[18]. Această derogare impune în prezent ca decizia automatizată să fie reexaminată cu o implicare umană semnificativă „cât mai curând posibil în mod rezonabil" după luarea deciziei[19].

22. Introducerea unor astfel de derogări ar putea prezenta un risc pentru drepturile și libertățile persoanelor vizate în absența unei monitorizări atente. În acest scop, cerința de reexaminare în timp util a derogării trebuie aplicată cu atenție pentru a evita lacunele în materie de supraveghere. Dacă criteriile pentru această implicare umană sunt interpretate prea vag sau revizuirea este întârziată, acest lucru ar putea duce la un control inadecvat și la diminuarea responsabilității. În acest context, CEPD reamintește jurisprudența Curții de Justiție a UE (CJUE), în special hotărârea Curții privind PNR, care a impus ca orice rezultat al sistemelor de creare automată de profiluri sau de corespondență să fie precedat de o verificare umană semnificativă și de substanță[20]. Poziția CJUE în ceea ce privește revizuirea umană prealabilă în contextul PNR oferă orientări importante referitoare la punerea în aplicare a garanțiilor privind procesul decizional automatizat prevăzute în LED. Întrucât o intervenție umană semnificativă este esențială pentru asigurarea respectării garanțiilor în procesul decizional automatizat, CEPD îndeamnă Comisia să includă în decizie evaluarea sa cu privire la această derogare nou introdusă și să monitorizeze punerea sa în aplicare din punct de vedere practic.

[16] A se vedea considerentul 46 din proiectul de decizie.
[17] A se vedea considerentul 66 din 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.
[18] Articolul 50C alineatul (4) litera (b) din DUAA.
[19] A se vedea și Department for Science, Innovation & Technology, Data (Use and Access) Act factsheet: UK GDPR and DPA [Ministerul Științei, Inovării și Tehnologiei, fișă de informare privind Legea privind datele (utilizarea și accesul)]: RGPD al Regatului Unit și DPA, publicat la 27 iunie 2025, p. 14, https://www.gov.uk/government/publications/data-use-and-access-act-2025-factsheets/data-use-and-access-act-factsheet-uk-gdpr-and-dpa.
[20] Hotărârea din 21 iunie 2022, C-817/19, EU:C:2022:491, punctul 179.

2.1.4 Cerințe privind înregistrarea

23. CEPD a reamintit în Recomandările sale 01/2021 că măsurile prevăzute într-un cadru de protecție a datelor dintr-o țară terță care permit unei autorități competente să își demonstreze conformitatea „ar trebui să includă păstrarea de evidențe sau înregistrări ale activităților de prelucrare a datelor pentru o perioadă de timp adecvată”[21]. În proiectul său de decizie, Comisia recunoaște că o astfel de obligație există în continuare în cadrul Regatului Unit, dar a fost modificată de DUAA, deoarece operatorul de date nu mai are obligația de a înregistra motivul specific al consultării sau al divulgării datelor cu caracter personal[22]. Eliminarea acestei obligații face excepție de la cerințele LED, care prevăd o înregistrare cuprinzătoare pentru a asigura transparența și responsabilitatea. LED se așteaptă la evidențe detaliate care să demonstreze prelucrarea legală, inclusiv justificarea accesului, pentru a facilita auditurile și a preveni utilizarea abuzivă. În cazul în care înregistrarea justificării în cadrul noului regim nu este obligatorie, ar putea deveni mai dificil să se verifice dacă datele au fost accesate în mod legal, atât în ceea ce privește operatorul, cât și autoritățile de supraveghere. CEPD invită Comisia să abordeze în continuare aceste cerințe reduse de înregistrare în decizia sa finală și să monitorizeze dacă această modificare afectează sau nu în mod negativ supravegherea și exercitarea drepturilor de către persoanele vizate.

2.1.5 Derogări din motive de securitate națională pentru autoritățile de aplicare a legii

24. Secțiunea 88 din DUAA actualizează derogările existente în materie de securitate națională în temeiul cadrului de aplicare a legii pentru a le reflecta pe cele disponibile în temeiul RGPD al Regatului Unit și al regimurilor serviciilor de informații[23]. Deși autoritățile de aplicare a legii sunt deja în măsură să restricționeze anumite obligații din motive de protecție a securității naționale – cum ar fi cele privind drepturile persoanelor vizate – secțiunea 78A din DPA din 2018[24] va include, de asemenea, majoritatea principiilor de protecție a datelor[25] și anumite cerințe internaționale privind transferul de date[26] ca dispoziții care pot fi înlăturate dacă acest lucru este necesar în scopul protejării securității naționale. În plus, unele competențe de intrare ale Comisarului pentru Informații de a efectua inspecții și de a lua măsuri de aplicare a legislației[27] pot fi înlăturate în aceste circumstanțe.

25. Aceste modificări nu sunt menționate nici în proiectul de decizie, nici în proiectul de decizie privind caracterul adecvat al nivelului de protecție în temeiul articolului 45 din RGPD. CEPD consideră însă că este esențial să se evalueze aceste derogări extinse în raport cu principiile necesității și proporționalității. În acest context, CEPD amintește cea de a doua dintre cele patru așa-numite „garanții esențiale europene”: orice limitare a exercitării drepturilor și libertăților recunoscute de Cartă trebuie să respecte esența acestora și, sub rezerva principiului proporționalității, poate fi impusă

[21] A se vedea considerentul 66 din 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.
[22] A se vedea considerentele 48 și 49 din proiectul de decizie.
[23] A se vedea și Department for Science, Innovation & Technology, Data (Use and Access) Act factsheet: UK GDPR and DPA [Ministerul Științei, Inovării și Tehnologiei, fișă de informare privind Legea privind datele (utilizarea și accesul)]: RGPD al Regatului Unit și DPA, publicat la 27 iunie 2025, p. 14, https://www.gov.uk/government/publications/data-use-and-access-act-2025-factsheets/data-use-and-access-act-factsheet-uk-gdpr-and-dpa.
[24] DUAA va fi introdusă treptat în mai multe etape. Principalele modificări ale legislației privind protecția datelor din partea 5 a DUAA vor intra în vigoare ca parte a etapei 3, la aproximativ 6 luni de la avizul regal, https://www.gov.uk/guidance/data-use-and-access-act-2025-plans-for-commencement.
[25] Secțiunea 78A alineatul (1), alineatul (2) litera (a) și alineatul (3) din Legea privind protecția datelor din 2018, astfel cum a fost introdusă prin secțiunea 88 din DUAA.
[26] Secțiunea 78A alineatul (1), alineatul (2) litera (d) și alineatul (4) din Legea privind protecția datelor din 2018, astfel cum a fost introdusă prin secțiunea 88 din DUAA.
[27] Secțiunea 78A alineatul (1), alineatul (2) literele (e), (f) și (g) din Legea privind protecția datelor din 2018, astfel cum a fost introdusă prin secțiunea 88 din DUAA.

numai dacă este necesară și răspunde într-adevăr obiectivelor de interes general recunoscute de Uniune sau necesității de a proteja drepturile și libertățile celorlalți[28]. CEPD își exprimă preocuparea cu privire la derogările de la principiile esențiale privind protecția datelor, la cerințele în materie de transferuri internaționale și la competențele Comisarului pentru Informații.

26. Potrivit normei revizuite, cinci din cele șase principii de protecție a datelor pot fi lăsate neaplicate când acest lucru este necesar pentru garantarea securității naționale[29]. Aceste principii stipulează, printre altele, că scopul de aplicare a legii pentru care sunt colectate datele cu caracter personal trebuie să fie specificat, explicit și legitim și că datele cu caracter personal trebuie să fie adecvate, relevante și neexcesive în raport cu acest scop. Ele mai precizează că datele cu caracter personal trebuie să fie exacte și păstrate numai cât timp este necesar. Astfel cum s-a menționat mai sus, viitoarele derogări includ, în plus, unele dintre cerințele privind transferurile internaționale, cum ar fi așa-numita a doua condiție pentru transferurile internaționale prevăzută în secțiunea 73 alineatul (3) din DPA din 2018. Această condiție impune ca transferurile să se bazeze pe reglementări privind caracterul adecvat al nivelului de protecție sau pe garanții adecvate, sau, dacă niciuna din ele nu se aplică, pe circumstanțe speciale. Derogările afectează, de asemenea, competențele Comisarului pentru Informații, de exemplu autoritatea de a emite notificări de informare și de executare[30].

27. CEPD ia act de faptul că, deși derogările se abat în mod clar de la LED, acestea sunt foarte asemănătoare cu derogările și restricțiile în materie de securitate națională prevăzute la articolul 11 din Convenția 108 modernizată a Consiliului Europei („Convenția 108+”)[31], pe care Regatul Unit a semnat-o la 10 octombrie 2018, dar care, la data prezentului aviz, nu a fost ratificată de Regatul Unit sau nu a intrat încă în vigoare[32]. În acest sens, CEPD reamintește Orientările privind principiile generale prevăzute la articolul 11 din Convenția 108+[33] emise recent de Comitetul Consultativ al Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (T-PD) a emis recent.

28. În orientările sale, Consiliul Europei subliniază în mod explicit că nu se aplică nicio excepție, printre altele, în ceea ce privește proporționalitatea și legitimitatea scopului principiilor de prelucrare. Acest lucru înseamnă că trebuie să se asigure proporționalitatea prelucrării datelor, precum și cerințele de prelucrare a datelor cu caracter personal într-un scop legitim. În conformitate cu Orientările T-PD, CEPD rămâne deosebit de vigilent în ceea ce privește orice derogare de la principiul proporționalității, precum și de la cerința de a prelucra datele cu caracter personal într-un scop legitim. De asemenea, în opinia CEPD, orice derogări de la competențele autorității de supraveghere trebuie abordate cu prudență. Deși cerințele specifice pentru activitățile de supraveghere – de exemplu autorizațiile de securitate – pot fi adecvate în contextul prelucrării datelor legate de securitatea națională, este esențial să se asigure o supraveghere eficientă pentru a preveni crearea unui vid de supraveghere. În

[28] Recomandările 02/2020 privind garanțiile esențiale europene pentru măsurile de supraveghere, adoptate la 10 noiembrie 2020, p. 10.

[29] În temeiul secțiunii 78A alineatele (2) și (3) din Legea privind protecția datelor din 2018, capitolul 2 din partea 3 a acestei legi nu se aplică dacă este necesar în scopul protejării securității naționale, cu excepția (a) secțiunii 35 alineatul (1) (primul principiu privind protecția datelor), în măsura în care impune ca prelucrarea datelor cu caracter personal să fie legală; (b) secțiunea 35 alineatele (2)-(5) (legalitatea prelucrării și restricții privind prelucrarea datelor sensibile); (c) secțiunea 42 (garanții: prelucrarea datelor sensibile) și (d) anexa 8 (condiții pentru prelucrarea datelor sensibile).

[30] Notificările de informare impun operatorului sau persoanei împuternicite de operator să furnizeze Comisarului informațiile necesare în mod rezonabil pentru îndeplinirea atribuțiilor sale. Notificările de executare împuternicesc Comisarul să solicite unei persoane să întreprindă (sau să se abțină de la a întreprinde) măsuri specifice, atunci când Comisarul este convins că persoana respectivă nu respectă anumite obligații în materie de protecție a datelor.

[31] Protocolul de modificare a Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (CETS nr. 223).

[32] https://www.coe.int/en-GB/web/conventions/full-list?module=signatures-by-treaty&treatynum=223.

[33] https://rm.coe.int/t-pd-2021-7rev13-interpretation-of-general-principles-article-11-c108-/1680b6c146.

același spirit, articolul 11 alineatul (3) din Convenția 108+ prevede că derogările de la articolul 15 din aceasta[34] „nu aduc atingere cerinței ca activitățile de prelucrare în scopuri de securitate națională și de apărare să facă obiectul unei revizuiri și unei supravegheri independente și eficace în temeiul legislației interne" ale părților la convenție. De asemenea, orice derogări trebuie interpretate cât mai restrictiv. Faptul că datele cu caracter personal sunt prelucrate în scopuri de securitate națională nu ar trebui să fie suficient în sine pentru invocarea unei derogări. Trebuie să fie clar că o derogare de la regimul de protecție a datelor trebuie să se aplice de la caz la caz și numai dacă acest lucru este necesar și proporțional[35].

29. Întrucât proiectele de decizii privind caracterul adecvat al nivelului de protecție nu abordează acest aspect, CEPD solicită Comisiei să își completeze evaluarea din proiectul de decizie, precum și să monitorizeze în mod specific aplicarea în practică a derogărilor în materie de securitate națională pentru autoritățile de aplicare a legii.

2.1.6 Exercitarea în comun a competenței de operator între serviciile de informații din Regatul Unit și autoritățile de aplicare a legii

30. Pe baza modificărilor efectuate de DUAA, activitățile de prelucrare desfășurate de autoritățile competente pentru asigurarea respectării legii pot intra, în anumite circumstanțe, sub incidența normelor aplicabile în mod normal prelucrării datelor cu caracter personal de către autoritățile naționale de securitate[36]. Cu alte cuvinte, sub rezerva condițiilor prevăzute în secțiunea 89 din DUAA, regimul de protecție a datelor în ceea ce privește prelucrarea în scopuri de securitate națională stabilit în partea 4 din DPA din 2018 este extins la prelucrarea datelor de către autoritățile de aplicare a legii.

31. Astfel cum este subliniat de către Comisie, condițiile prevăzute în secțiunea 89 din DUAA oferă garanții stricte: o autoritate competentă trebuie să fie specificată ca „autoritate competentă calificată" în reglementările adoptate de secretarul de stat, care, în plus, trebuie să desemneze o anumită activitate de prelucrare efectuată de autoritatea competentă calificată drept operator asociat cu cel puțin un serviciu de informații în scopul protejării securității naționale[37].

32. Deși recunoaște că aceste garanții implică restricții semnificative, CEPD invită Comisia să monitorizeze aplicarea practică a acestor norme. Ar trebui să se acorde o atenție deosebită asigurării faptului că partea 4 din DPA din 2018 se aplică strict operațiunilor de prelucrare în scopuri de securitate națională, fără a fi extinsă la alte contexte. Deși statelor li se acordă o marjă largă de apreciere în materie de securitate națională, astfel cum a recunoscut și Curtea Europeană a Drepturilor Omului[38], CEPD consideră că amenințările la adresa securității naționale trebuie să poată fi diferențiate prin natura lor, prin gravitatea lor și prin circumstanțele specifice de riscurile generale pentru siguranța publică sau de

[34] Articolul 15 din Convenția 108+ precizează modul în care părțile la convenție, prevăzând una sau mai multe autorități de supraveghere, asigură respectarea dispozițiilor convenției.

[35] A se vedea și articolul 11 din Convenția 108+, care precizează că excepțiile trebuie să fie prevăzute de lege, să respecte esența drepturilor și libertăților fundamentale și să constituie o măsură necesară și proporțională într-o societate democratică. Potrivit Orientărilor TP-D privind principiile generale ale articolului 11, aceasta implică faptul că trebuie efectuată o evaluare a intereselor implicate între necesitatea de a prevedea derogări de la anumite dispoziții ale Convenției și respectarea drepturilor omului și a libertăților fundamentale ale persoanelor fizice, iar această evaluare trebuie să fie justificată.

[36] A se vedea considerentul 72 din proiectul de decizie de punere în aplicare a Comisiei în temeiul Regulamentului (UE) 2016/679, care este la fel de relevant pentru ambele avize ale CEPD în această privință (a se vedea, de asemenea, secțiunea 4 de mai sus).

[37] A se vedea considerentul 73 din proiectul de decizie de punere în aplicare a Comisiei în temeiul Regulamentului (UE) 2016/679, care este la fel de relevant pentru ambele avize ale CEPD în această privință (a se vedea, de asemenea, secțiunea 4 de mai sus).

[38] CEDO, Big Brother Watch și alții/Regatul Unit, 25 mai 2021, punctul 350.

infracțiunile grave. Numai în aceste cazuri funcționarea autorităților de aplicare a legii în cadrul regimului de protecție a datelor al serviciilor de informații este compatibilă cu principiile necesității și proporționalității[39]. În plus, CEPD consideră că trebuie monitorizat dacă autoritățile competente calificate sunt capabile, în practică, să mențină o distincție clară între diferitele scopuri ale prelucrării, pentru a respecta cadrul juridic corespunzător.

2.1.7 Dreptul de acces

33. DUAA precizează că persoanele vizate au dreptul la informațiile relevante numai dacă operatorul este în măsură să le furnizeze pe baza unei căutări rezonabile și proporționale. Această modificare este introdusă atât în regimul de aplicare a legii, cât și în regimul de securitate națională[40].

34. Comisia explică acest lucru ca o clarificare în conformitate cu standardele consacrate elaborate în temeiul jurisprudenței interne, care iau în considerare și interesele persoanei vizate. Cu toate acestea, CEPD ar fi apreciat transmiterea unor informații mai detaliate cu privire la modul în care este interpretată noțiunea de „căutare rezonabilă și proporțională", inclusiv deoarece articolul 14 din LED nu conține un astfel de element. CEPD recunoaște că pot exista într-adevăr scenarii în care eforturile unui operator de a identifica și a localiza informații cu privire la persoana vizată ar putea fi considerate nerezonabile și disproporționate, fără a compromite echivalența esențială[41]. Cu toate acestea, este important să se definească în mod adecvat noțiunea de „căutare rezonabilă și proporțională", care, în opinia CEPD, ar trebui interpretată în sens restrictiv și într-un mod suficient de uniform. Autoritățile competente ar trebui să înțeleagă în mod consecvent ce este „rezonabil și proporțional", indiferent dacă se bazează pe jurisprudență sau pe orientări din partea unei autorități de supraveghere, deoarece aplicarea acestei noțiuni ar putea conduce la standarde diferite în ceea ce privește respectarea dreptului de acces, în special în funcție de nivelul măsurilor tehnice și organizatorice pe care operatorul le-a instituit pentru a trata cererile de acces. CEPD invită Comisia să monitorizeze faptul că dreptul de acces nu este limitat în mod nejustificat.

2.1.8 Supravegherea și căile de atac

35. CEPD ia act de faptul că sistemul de supraveghere a agențiilor de aplicare a dreptului penal în temeiul DPA din 2018 și al Legii privind competențele de investigare din 2016, precum și mecanismele de recurs, disponibile în temeiul părții 3 din DPA din 2018, al Legii privind competențele de investigare din 2016 și al Legii privind drepturile omului din 1998, rămân în mare măsură neschimbate. În special, supravegherea în Regatul Unit continuă să fie asigurată, în afară de Biroul Comisarului pentru Informații (*Information Commissioner's Office* – „ICO"), de o combinație de diferiți comisari, și anume Comisarul pentru Competențe de Investigare (*Investigatory Powers Commissioner* – „IPC"), asistat de alți comisari judiciari, precum și Comisarul pentru Biometrie și Camere de Supraveghere.

36. După cum explică Comisia în considerentul 97 din proiectul de decizie, Legea din 2024 de modificare a competențelor de investigare a adus doar modificări limitate, în special prin introducerea de IPC adjuncți cărora IPC le poate delega competențe specifice atunci când aceștia nu sunt în măsură sau nu

[39] Din jurisprudența CJUE rezultă că, atunci când se aplică testul de necesitate și proporționalitate legislației statelor membre care permite păstrarea și accesul autorităților publice la datele cu caracter personal, obiectivele legitime, cum ar fi securitatea națională sau combaterea infracțiunilor grave, sunt diferite și, prin urmare, ar putea justifica tipuri diferite de ingerință. A se vedea CJUE, cauzele conexate C-511/18, C-512/18 și C-520/18, La Quadrature du Net și alții, 6 octombrie 2020.
[40] Secțiunea 78 alineatele (3) și (4) din DUAA, care modifică articolele 45 și 94 din Legea privind protecția datelor din 2018.
[41] De exemplu, s-ar putea argumenta că acesta este cazul efectuării de căutări pe dispozitivele confiscate care nu au fost încă analizate sau decriptate.

sunt disponibili să își îndeplinească funcțiile. IPC adjuncți trebuie să fie comisari judiciari și sunt numiți de IPC.

37. CEPD constată cu satisfacție că ideile anterioare din proiectul de lege privind protecția datelor și informațiile digitale, care a precedat DUUA, de a desființa funcția de Comisar pentru Biometrie și Camere de Supraveghere și de a transfera rolul acestuia Comisarului pentru Competențe de Investigare, au fost abandonate[42]. În acest sens, CEPD invită Comisia să acorde mai multă atenție acestui aspect și să furnizeze o evaluare mai detaliată a rolului Comisarului pentru Biometrie și Camere de Supraveghere în sistemul de supraveghere în cursul monitorizării sale și al viitoarelor revizuiri ale proiectului de decizie.

38. Astfel cum a subliniat deja CEPD în Avizul 14/2021, ICO dispune de competențele necesare, care corespund îndeaproape competențelor autorităților de supraveghere din statele membre ale UE, astfel cum sunt prevăzute la articolul 58 din RGPD. În același timp, astfel cum a subliniat deja CEPD, existența unor sancțiuni eficace joacă un rol important în asigurarea respectării normelor[43].

39. CEPD ia act cu satisfacție de politica de transparență a ICO și de disponibilitatea datelor statistice și analitice, inclusiv a exemplelor, ale activităților ICO de asigurare a respectării legii în raport cu organismele de aplicare a legii[44]. În acest sens, CEPD observă o preferință a autorității de supraveghere din Regatul Unit pentru emiterea de avertismente în cazul încălcării legislației privind protecția datelor de către forțele de poliție. O excepție notabilă este reprezentată de notificarea de executare emisă către Ministerul Public în ianuarie 2024[45]. CEPD consideră, de asemenea, pozitiv faptul că, de la adoptarea Deciziei de punere în aplicare 2021/1773, ICO a publicat numeroase coduri de bune practici, orientări, avize și alte documente de orientare pentru părțile relevante.

40. CEPD ia act, de asemenea, de faptul că, odată cu intrarea în vigoare a DUAA, supravegherea independentă a ICO, structurată anterior ca o întreprindere individuală, va fi transformată într-o nouă structură prin introducerea unui organism constituit ca entitate juridică, și anume Comisia pentru Informații[46].

41. CEPD furnizează o analiză inițială a posibilelor implicații ale acestei modificări în Avizul său 26/2025 privind proiectul de decizie de punere în aplicare a Comisiei în temeiul Regulamentului (UE) 2016/679 privind protecția adecvată a datelor cu caracter personal în Regatul Unit. Observațiile și recomandările din avizul respectiv sunt pe deplin valabile și în contextul supravegherii și supervizării în domeniul asigurării respectării legii.

42. În special, CEPD invită Comisia să completeze proiectul de decizie privind caracterul adecvat al nivelului de protecție cu detalii suplimentare, în special cu privire la structura și organizarea Comisiei pentru Informații, numirea și revocarea membrilor Comisiei pentru Informații, mai ales cu privire la numirea membrilor neexecutivi ai Comisiei pentru Informații de către secretarul de stat. CEPD consideră, de asemenea, că, în viitoarele sale revizuiri, Comisia ar trebui să acorde o atenție deosebită echilibrării de către Comisia pentru Informații a diferitelor sarcini și interese. În plus, CEPD invită Comisia să dea curs

[42] A se vedea https://www.gov.uk/government/organisations/biometrics-and-surveillance-camera-commissioner.
[43] Avizul CEPD 14/2021, punctul 112.
[44] A se vedea, de exemplu, seturile de date detaliate privind plângerile referitoare la protecția datelor, disponibile la adresa https://ico.org.uk/action-weve-taken/complaints-and-concerns-data-sets/data-protection-complaints/
[45] https://ico.org.uk/action-weve-taken/enforcement/crown-prosecution-service-1/.
[46] A se vedea noul articol 114a din DPA din 2018 și secțiunea 6 din DUAA.

rezultatelor consultării publice publicate de ICO la 22 august 2025 cu privire la tratarea plângerilor[47] și să monitorizeze politicile rezultate ale Comisiei pentru Informații.

43. Având în vedere cele de mai sus, CEPD reiterează necesitatea monitorizării îndeaproape de către Comisie a aplicării competențelor corective și a căilor de atac pentru părțile afectate în cadrul de protecție a datelor din Regatul Unit.

3 REVIZUIREA, DURATA ȘI REÎNNOIREA DECIZIEI

44. CEPD ia act de faptul că prezentul proiect de decizie se aplică timp de șase ani, cu data de expirare stabilită pentru 27 decembrie 2031, și ia act de faptul că Regatul Unit continuă să fie singura țară terță ale cărei decizii privind caracterul adecvat al nivelului de protecție conțin o clauză de caducitate. CEPD înțelege că noul cadru juridic merită o atenție deosebită și invită Comisia să monitorizeze cu atenție punerea în aplicare a DUAA, inclusiv domeniile de interes evidențiate în prezentul aviz și toate evoluțiile relevante din Regatul Unit în această privință. CEPD ia act, de asemenea, de faptul că „clauza de caducitate" este combinată cu revizuirea periodică obligatorie prevăzută la articolul 36 alineatul (3) din LED, care ar trebui să aibă loc cel puțin o dată la patru ani.

45. CEPD înțelege că intenția Comisiei este de a efectua o revizuire la sfârșitul perioadei de patru ani, pe baza căreia va întocmi un raport public. CEPD consideră binevenită intenția de a efectua revizuirea, care servește unui scop diferit de clauza de caducitate și îndeplinește un rol important în monitorizarea cadrului juridic, în special în ceea ce privește responsabilitatea. Prin urmare, CEPD îndeamnă Comisia să efectueze revizuirea în termenul legal specificat la articolul 36 alineatul (3) din LED, ținând seama, de asemenea, de elementele deja prezentate în Decizia de punere în aplicare 2021/1773 a Comisiei[48], precum și de orice alte evoluții ulterioare relevante.

46. În plus, CEPD înțelege că analiza din Decizia de punere în aplicare 2021/1773 a Comisiei privind suspendarea și abrogarea deciziei[49] este încă valabilă. Din motive de securitate juridică, CEPD consideră că o astfel de clarificare ar putea apărea în decizia finală privind caracterul adecvat al nivelului de protecție.

47. CEPD apreciază faptul că considerentul 68 din proiectul de decizie se referă la rolul CEPD, precum și al grupurilor societății civile și al altor părți interesate în mecanismul de revizuire periodică, în conformitate cu Recomandările CEPD 01/2021[50]. În ceea ce privește implicarea practică a CEPD și a reprezentanților săi în pregătirea și desfășurarea revizuirilor viitoare, CEPD reiterează că orice documentație relevantă ar trebui comunicată în scris CEPD cu suficient timp înainte de desfășurarea revizuirilor.

[47] https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/2025/08/ico-consultation-on-draft-changes-to-how-we-handle-data-protection-complaints/; https://ico.org.uk/media2/nrljbhr2/proposed-dpt-framework-20250822.pdf.
[48] A se vedea considerentele 165-167 din Decizia de punere în aplicare 2021/1773 a Comisiei.
[49] Ibidem, considerentele 168-171.
[50] Considerentul 19 din 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.

48. Având în vedere caracteristicile specifice ale prezentului proiect de decizie, CEPD invită Comisia să detalieze și să clarifice într-o măsură cât mai mare elementele referitoare la durata, monitorizarea, suspendarea, revocarea, modificarea și reînnoirea deciziei.

Pentru Comitetul European pentru Protecția Datelor

Președinte

Anu Talus