Avizul 07/2025 privind Proiectul de decizie de punere în aplicare a Comisiei Europene în temeiul Regulamentului (UE) 2016/679 privind protecția adecvată a datelor cu caracter personal de către Organizația Europeană de Brevete

Adoptat la 5 mai 2025

Rezumat

La 4 martie 2025, Comisia Europeană a demarat procesul de adoptare a proiectului său de decizie de punere în aplicare (proiectul de decizie) privind protecția adecvată a datelor cu caracter personal de către Organizația Europeană de Brevete (OEB sau organizația)[1].

La 5 martie 2025, Comisia Europeană a solicitat avizul Comitetului european pentru protecția datelor (CEPD). Evaluarea efectuată de CEPD privind caracterul adecvat al nivelului de protecție asigurat de Organizația Europeană de Brevete a fost realizată în baza examinării proiectului de decizie ca atare, precum și în baza analizării documentației puse la dispoziție de Comisia Europeană.

CEPD s-a concentrat pe evaluarea cadrului juridic și a normelor privind protecția datelor aplicabile Organizației Europene de Brevete, precum și a căilor de atac aflate la dispoziția persoanelor fizice din Spațiul Economic European (SEE), inclusiv accesul autorităților publice la datele cu caracter personal transferate din SEE către Organizația Europeană de Brevete.

CEPD a evaluat, de asemenea, dacă garanțiile prevăzute în cadrul juridic al Organizației Europene de Brevete sunt în vigoare și eficace și și-a axat evaluarea în special pe supraveghere și aplicare, ținând seama de specificul organizațiilor internaționale.

CEPD a utilizat ca referință principală pentru această activitate criteriile de referință privind caracterul adecvat al nivelului de protecție adoptate de Grupul de lucru „Articolul 29”[2].

CEPD constată cu satisfacție că există numeroase similitudini între cadrul de protecție a datelor al Organizației Europene de Brevete și cadrul de protecție a datelor al Uniunii Europene, inclusiv în ceea ce privește drepturile și principiile în materie de protecție a datelor.

De asemenea, a concluzionat că anumite aspecte ar trebui clarificate în continuare și monitorizate îndeaproape de Comisia Europeană.

În special, CEPD invită Comisia să clarifice că, în contextul structurii de guvernanță a protecției datelor implementate de Organizația Europeană de Brevete, operatorul (adică Oficiul European de Brevete) rămâne entitatea responsabilă în ultimă instanță pentru încălcările normelor în materie de protecție a datelor.

În ceea ce privește transferurile ulterioare, CEPD observă că cerința de a nu submina nivelul de protecție nu este menționată în mod expres în legătură cu așa-numitele „transmiteri” de date cu caracter personal către autoritățile publice din statele contractante ale Organizației Europene de Brevete. CEPD solicită Comisiei să clarifice acest aspect și ce garanții se aplică atunci când datele cu caracter personal sunt transmise în contextul specific al procedurii de acordare a brevetelor.

Având în vedere legătura strânsă dintre responsabilul cu protecția datelor (RPD) și Comitetul pentru protecția datelor (CPD), precum și importanța competențelor de investigare, de audit și corective, CEPD recomandă Comisiei să clarifice în continuare interacțiunea dintre acestea, în special în ceea ce privește exercitarea competențelor de investigare, de audit și corective, precum și să clarifice rolul RPD-ului în tratarea cererilor persoanelor vizate și rolul său, dacă este cazul, în procedura de depunere a plângerilor la CPD. În plus, CEPD observă că avizele (motivate) emise de CPD în contextul procedurii de depunere a plângerilor sunt în continuare neobligatorii și invită Comisia să verifice și să se asigure

[1] Comunicat de presă https://ec.europa.eu/commission/presscorner/detail/sv/ip_25_613.

[2] Grupul de lucru „Articolul 29”, WP 254 rev. 01, adoptat la 28 noiembrie 2017 și revizuit ultima dată și adoptat la 6 februarie 2018, aprobat de CEPD.

că în acest context competențele CPD-ului sunt obligatorii și să evalueze dacă ar putea fi prevăzute garanții suplimentare în acest sens.

CEPD a analizat, de asemenea, cadrul juridic al Organizației Europene de Brevete în ceea ce privește accesul autorităților publice la datele cu caracter personal transferate din Uniune către organizație și utilizarea acestora. În acest sens, CEPD subliniază că evaluarea accesului autorităților publice în cazul de față este distinctă de evaluarea care corespunde nivelului de protecție oferit de o țară terță. Scenariul specific al unei decizii privind protecția adecvată a datelor cu caracter personal de către o organizație internațională necesită revizuirea normelor care determină modul în care organizația respectivă tratează cererile de acces ale autorităților publice.

În ceea ce privește statele contractante, imunitățile Organizației Europene de Brevete sunt completate de o obligație de cooperare. În acest scop, Organizația Europeană de Brevete poate renunța la imunitatea sa de jurisdicție și de executare pentru a răspunde cererilor de acces ale autorităților publice. CEPD invită Comisia să clarifice în continuare, în special în ceea ce privește cererile de acces în scopuri de aplicare a legii și de securitate națională, modul în care obligația de cooperare se raportează la conceptul de imunitate. În acest context, CEPD invită Comisia să clarifice, de asemenea, autoritatea președintelui și puterea sa discreționară atunci când decide cu privire la o cerere de cooperare.

Dacă Organizația Europeană de Brevete decide să dea curs unei cereri de acces din partea unui stat contractant, se aplică cerințele privind transmiterea datelor. Aceste norme se aplică tuturor statelor contractante, indiferent dacă statul contractant este un stat membru al SEE sau este considerat țară terță din perspectiva legislației UE privind protecția datelor. CEPD subliniază că cerințele din capitolul V din RGPD, în măsura în care este necesar pentru a stabili nivelul de protecție în esență echivalent, trebuie abordate în mod suficient și invită Comisia să clarifice ce garanții se aplică în astfel de cazuri.

Cuprins

Comitetul european pentru protecția datelor,

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

având în vedere Acordul privind Spațiul Economic European (SEE), în special anexa XI și Protocolul 37 la acesta, astfel cum au fost modificate prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018[3],

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

ADOPTĂ URMĂTORUL AVIZ:

1. INTRODUCERE

1. Capitolul V din RGPD stabilește condițiile pentru transferul datelor cu caracter personal către o țară terță sau către o organizație internațională. Transferurile de date cu caracter personal pot avea loc pe baza unei decizii privind caracterul adecvat al nivelului de protecție a Comisiei Europene (articolul 45 din RGPD) sau, în absența unei astfel de decizii, în cazul în care operatorul sau persoana împuternicită de operator oferă garanții adecvate, inclusiv drepturi opozabile și căi de atac legale pentru persoana vizată (articolul 46 din RGPD). În lipsa unei decizii privind caracterul adecvat al nivelului de protecție sau a unor garanții adecvate, un transfer sau o serie de transferuri către o țară terță sau o organizație internațională au loc numai în anumite condiții (articolul 49 din RGPD).

2. CEPD reamintește că deciziile privind caracterul adecvat al nivelului de protecție asigură protecția continuă a datelor cu caracter personal transferate din SEE către țări terțe și constituie un instrument solid de transfer pentru a garanta protejarea drepturilor persoanei vizate atunci când datele sunt transferate în afara SEE.

3. În special, CEPD salută inițiativa Comisiei de a lucra la prima decizie privind caracterul adecvat al nivelului de protecție pentru o organizație internațională și subliniază importanța acestei decizii pentru a demonstra că se poate recunoaște că cadrul juridic al organizațiilor internaționale asigură un nivel adecvat de protecție în sensul articolului 45 din RGPD.

4. CEPD profită de această ocazie pentru a încuraja Comisia să continue dialogul cu organizațiile internaționale în vederea dezvoltării, a extinderii și a multiplicării acestui tip de decizii privind caracterul adecvat al nivelului de protecție, pe lângă cele referitoare la țările terțe.

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

1.1 Structura și cadrul legal privind protecția datelor al Organizației Europene de Brevete

5. Organizația Europeană de Brevete, cu sediul la München, este o organizație interguvernamentală înființată prin Convenția brevetului european (CBE)[4]. Are 39 de state contractante și deține personalitate juridică. Este alcătuită din două organe principale: Oficiul European de Brevete (Oficiul), care funcționează ca ramură executivă, și Consiliul de administrație, care exercită atribuții legislative în numele Organizației Europene de Brevete și este responsabil pentru chestiunile de politică (articolul 33 din CBE).

6. Principala competență a Organizației Europene de Brevete este acordarea de brevete europene, sarcină îndeplinită de Oficiu sub supravegherea Consiliului de administrație.

7. Președintele reprezintă Organizația Europeană de Brevete și este șeful Oficiului, care include diverse departamente. Președintele este responsabil de gestionarea operațiunilor Oficiului și de chestiunile disciplinare și răspunde în fața Consiliului de administrație. Consiliul de administrație este format din reprezentanți ai statelor contractante, supraveghează chestiunile de politică și activitățile Oficiului.

8. La 30 iunie 2021, Organizația Europeană de Brevete a adoptat Normele privind protecția datelor, care implementează articolele 1B și 32A din Statutul personalului[5] și se aplică prelucrării datelor cu caracter personal de către Oficiu[6].

9. Normele privind protecția datelor sunt completate de instrumente emise de președinte, în special circulare, instrucțiuni administrative interne și decizii [cum ar fi Decizia privind țările și entitățile care asigură o protecție adecvată a datelor (17 noiembrie 2022) și *Circulara nr. 420 de punere în aplicare a articolului 25 din Normele privind protecția datelor privind restricționarea drepturilor persoanelor vizate*]. Toate aceste instrumente sunt obligatorii din punct de vedere juridic[7].

10. Normele privind protecția datelor sunt completate în continuare de documente operaționale emise de responsabilul cu protecția datelor, care specifică cerințe și proceduri mai detaliate pentru prelucrarea datelor cu caracter personal [articolul 1 alineatul (2) litera (c) din Normele privind protecția datelor]. Aceste documente operaționale fac parte din cadrul legal privind protecția datelor al Organizației Europene de Brevete și, ca atare, sunt obligatorii din punct de vedere juridic și sunt puse la dispoziția persoanelor vizate pe site-ul Organizației Europene de Brevete.

[4] Considerentul 7 din proiectul de decizie.

[5] Statutul personalului reglementează aspecte legate de personalul Organizației Europene de Brevete, inclusiv drepturile și obligațiile personalului. Vezi în acest sens articolul 33 din CBE. CBE este disponibilă la următorul link: https://link.epo.org/web/EPC_17th_edition_2020_en.pdf.

[6] Prelucrarea datelor cu caracter personal efectuată de Consiliul de administrație al Organizației Europene de Brevete este reglementată de Normele privind protecția datelor ale Consiliului de administrație, în timp ce prelucrarea datelor cu caracter personal efectuată de Comitetul restrâns este reglementată de Normele privind protecția datelor ale Comitetului restrâns. Normele privind protecția datelor ale Consiliului de administrație și, respectiv, Normele privind protecția datelor ale Comitetului restrâns stabilesc aplicarea Normelor privind protecția datelor la prelucrarea datelor cu caracter personal efectuată de Consiliul de administrație și de Comitetul restrâns, cu modificările necesare. Articolul 145 din CBE clarifică rolul Comitetului restrâns.

[7] Articolul 10 din CBE, articolul 1 alineatul (2) litera (a) din Normele privind protecția datelor și articolul 3 litera (y) din Normele privind protecția datelor.

1.2 Specificul organizațiilor internaționale

11. În conformitate cu articolul 4 punctul 26 din RGPD, o organizație internațională înseamnă „o organizație și organismele sale subordonate reglementate de dreptul internațional public sau orice alt organism care este instituit printr-un acord încheiat între două sau mai multe țări sau în temeiul unui astfel de acord”. În temeiul dreptului internațional, statutul organizațiilor internaționale este similar cu cel al statelor suverane; cu toate acestea, în conformitate cu principiul imunității funcționale, organizațiile internaționale beneficiază de privilegii și imunități numai în măsura în care este necesar pentru exercitarea funcțiilor pentru care au fost create[8]. „Privilegiile” includ, în general, scutiri de la aplicarea dreptului material al unui stat (de exemplu, scutiri fiscale și vamale), iar „imunitățile” sunt scutiri de la proceduri judiciare, măsuri de executare și de aplicare a legii.

12. Sursele privilegiilor și imunităților organizațiilor internaționale pot fi: tratate multilaterale, acorduri internaționale de înființare a organizației internaționale, acorduri privind sediul central cu statul gazdă, precum și legislația și dreptul intern. Privilegiile și imunitățile sunt de obicei recunoscute de statele membre ale organizațiilor, cu excepția cazului în care țări terțe au recunoscut explicit sau implicit organizația internațională în dreptul intern. Cu toate acestea, imunitatea față de jurisdicția națională nu este absolută și impune ca persoanele fizice să dispună de mijloace alternative rezonabile pentru a-și proteja în mod eficient drepturile[9].

1.3 Privilegiile și imunitățile Organizației Europene de Brevete

13. Privilegiile și imunitățile de care beneficiază Organizația Europeană de Brevete sunt reglementate de *Protocolul privind privilegiile și imunitățile Organizației Europene de Brevete* (PPI) și se referă, printre altele, la sediul Organizației Europene de Brevete (articolul 1); inviolabilitatea arhivelor (articolul 2 din PPI); jurisdicția și executarea [articolul 3 alineatul (1) litera (a) din PPI], proprietatea și activele Organizației Europene de Brevete: cu excepția cazurilor în care acest lucru este temporar necesar în legătură cu prevenirea și investigarea accidentelor care implică autovehicule aparținând organizației sau operate în numele acesteia. [articolul 3 alineatul (3) din PPI]; scutirea fiscală (articolul 4 din PPI).

14. Imunitățile Organizației Europene de Brevete sunt completate de o obligație de cooperare între Organizația Europeană de Brevete și autoritățile publice ale statelor contractante, astfel cum se prevede la articolul 20 din PPI. În plus, în conformitate cu articolul 19 alineatul (2), președintele Oficiului European de Brevete are obligația de a renunța la imunitate în cazul în care consideră că aceasta împiedică desfășurarea normală a justiției și că este posibil să se renunțe la această imunitate fără a prejudicia interesele organizației.

[8] Christopher Kuner: „International Organizations and the EU General Data Protection Regulation” (Organizațiile internaționale și Regulamentul general al UE privind protecția datelor), Facultatea de Drept a Universității din Cambridge, Seria de studii de cercetări juridice, Studiul 20/2018.

[9] Waite și Kennedy împotriva Germaniei, CEDO, cererea nr. 26083/94, hotărârea din 18 februarie 1999, punctele 67-73.

1.4 Guvernanța protecției datelor în cadrul Organizației Europene de Brevete

15. În conformitate cu articolul 3 litera (g) din Normele privind protecția datelor, Oficiul European de Brevete are rolul de operator[10]. Cadrul legal privind protecția datelor al Organizației Europene de Brevete prevede posibilitatea ca operatorul să identifice unitățile operaționale ca „operatori delegați" [articolul 28 alineatul (3) din Normele privind protecția datelor]. În conformitate cu articolul 3 litera (h) din Normele privind protecția datelor, „operator delegat înseamnă unitatea operațională, reprezentată de conducătorul său, care se asigură că toate operațiunile de prelucrare a datelor cu caracter personal efectuate în cadrul unității operaționale respectă prezentele norme. Persoana care reprezintă unitatea este director de nivel superior, de obicei cel puțin un director principal."

16. CEPD observă că această structură de guvernanță internă este comună în contextul organizațiilor internaționale[11], având în vedere amploarea și natura activității lor. În mod similar, companiile beneficiază de o structură internă care sprijină respectarea normelor privind protecția datelor[12].

17. CEPD observă însă că responsabilitatea finală în cazul încălcării normelor privind protecția datelor ar trebui să revină operatorului (adică Oficiului European de Brevete)[13]. Având în vedere cele de mai sus, CEPD invită Comisia să clarifice în continuare acest aspect.

2. ASPECTE GENERALE PRIVIND PROTECȚIA DATELOR

2.1 Principii privind conținutul

18. Capitolul 3 din Criteriile de referință privind caracterul adecvat al nivelului de protecție este dedicat „Principiilor privind conținutul" și se referă la conceptele și principiile de bază ale protecției datelor. Sistemul unei țări terțe sau al unei organizații internaționale trebuie să conțină astfel de concepte și principii de bază pentru a asigura un nivel de protecție a datelor cu caracter personal în esență echivalent cu cel garantat de legislația UE. Acestea nu trebuie să redea întocmai terminologia RGPD, însă ar trebui să reflecte conceptele consacrate în legislația UE privind protecția datelor și să fie în concordanță cu acestea. Criteriile de referință privind caracterul adecvat al nivelului de protecție fac referire la următoarele concepte importante: „date cu caracter personal", „prelucrare", „operatori de date", „persoană împuternicită de operator ", „destinatar" și „date sensibile".

19. CEPD salută recunoașterea drepturilor la viață privată și la protecția datelor ca drepturi fundamentale în conformitate cu Normele privind protecția datelor.

---

[10] Articolul 28 din Normele privind protecția datelor detaliază mai bine competența de operator în cadrul Organizației Europene de Brevete.

[11] De exemplu, Regulamentul Eurocontrol privind protecția datelor face referire la „operatori interni" https://www.eurocontrol.int/sites/default/files/2024-05/eurocontrol-regulation-personal-data-protection-2024.pdf; BEI utilizează termenul „operator" atât pentru operatorii delegați, cât și pentru BEI, dar textul face adesea referire la „operatorii relevanți", precizând clar că aceștia se referă la o entitate specifică din cadrul BEI, documentul fiind disponibil la adresa https://www.eib.org/attachments/lucalli/20220237_data_protection_rules_implementing_eu_regulation_en.pdf

[12] Orientările 07/2020 privind conceptele de operator și persoană împuternicită de operator în cadrul RGPD, versiunea 2.1, adoptate la 7 iulie 2021.

[13] *Ibid*., punctele 17 și 18.

2.1.1 Concepte

20. CEPD recunoaște că terminologia utilizată în cadrul legal privind protecția datelor al Organizației Europene de Brevete este în concordanță cu cea utilizată în cadrul legal privind protecția datelor al UE. Această aliniere este un factor pozitiv care, deși nu constituie o condiție prealabilă pentru echivalență, merită erecunoaștere.

21. În ceea ce privește conceptele de „operator delegat" și de „unitate operațională" și consecințele lor practice, CEPD face referire la secțiunea 1.4 de mai sus.

2.1.2 Principiile în materie de protecție a datelor

22. Principiile în materie de protecție a datelor prevăzute la articolul 4 alineatul (2) și la articolul 6 din Normele privind protecția datelor sunt similare cu cele prevăzute la articolul 5 și, respectiv, articolul 6 alineatul (4) din RGPD. În mod similar, temeiurile juridice pentru prelucrare prevăzute la articolele 5, 7, 11 și 12 din Normele privind protecția datelor reflectă temeiurile juridice prevăzute la articolul 6 din RGPD și condițiile prevăzute la articolele 9 și 10 din RGPD[14].

23. În conformitate cu articolul 11 alineatul (2) din Normele privind protecția datelor, categoriile speciale de date cu caracter personal pot fi prelucrate în condiții similare cu cele prevăzute la articolul 9 din RGPD, cu excepția anumitor cazuri care decurg din natura Organizației Europene de Brevete. În temeiul articolului 11 alineatul (2) litera (f) din Normele privind protecția datelor, de exemplu, aceste date pot fi prelucrate atunci când este necesar pentru un scop specific legat de îndeplinirea unei sarcini efectuate în exercitarea activităților oficiale ale organizației sau în exercitarea legitimă a autorității publice cu care este investit operatorul.

24. În astfel de cazuri, însă, articolul 11 alineatul (2) litera (f) din Normele privind protecția datelor prevede măsuri specifice pentru a se asigura că nivelul de protecție al categoriilor speciale de date cu caracter personal nu este afectat.

25. CEPD salută faptul că, în ceea ce privește principiul limitărilor legate de scop, compatibilitatea scopurilor ulterioare este înțeleasă în mod similar atât la articolul 4 alineatul (2) litera (b) și articolul 6 din Normele privind protecția datelor, cât și la articolul 5 alineatul (1) litera (b) și articolul 6 alineatul (4) din RGPD.

26. În plus, CEPD salută includerea principiului responsabilității la articolul 4 alineatul (1) din Normele privind protecția datelor, precum și a măsurilor necesare pentru a demonstra conformitatea, cum ar fi păstrarea înregistrărilor (articolul 32), obligațiile de notificare a încălcării securității datelor (articolul 34), evaluarea impactului asupra protecției datelor (articolul 38 din Normele privind protecția datelor), precum și includerea protejării vieții private începând cu momentul conceperii și în mod implicit [articolul 27 alineatele (1) și (2) din Normele privind protecția datelor], care asigură, de asemenea, respectarea principiilor reducerii la minimum a datelor și al necesității. CEPD constată cu satisfacție că aceste principii și obligații sunt similare cu cele prevăzute în RGPD.

27. În plus, CEPD apreciază că articolul 4 alineatul (1) din Normele privind protecția datelor prevede că operatorul trebuie să pună în aplicare în mod activ și continuu măsuri pentru a asigura protecția datelor cu caracter personal în cadrul activităților sale de prelucrare, responsabilizându-l astfel pentru respectarea legislației în materie de protecție a datelor și impunându-i să demonstreze această conformitate persoanelor vizate în orice moment.

[14] Vezi considerentele 26-29 din proiectul de decizie.

2.2 Drepturi individuale

28. CEPD apreciază că Normele privind protecția datelor oferă persoanelor fizice aceleași drepturi ca cele prevăzute în RGPD (articolele 12-22), și anume dreptul de acces (articolul 18 din Normele privind protecția datelor), dreptul la rectificare (articolul 19 din Normele privind protecția datelor), dreptul la ștergere (articolul 20 din Normele privind protecția datelor), dreptul la restricționarea prelucrării (articolul 21 din Normele privind protecția datelor), dreptul la portabilitatea datelor (articolul 22 din Normele privind protecția datelor), dreptul la opoziție (articolul 23 din Normele privind protecția datelor) și dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată (articolul 24 din Normele privind protecția datelor). În același mod, dreptul de a fi informat cu privire la restricționarea drepturilor persoanei vizate [articolul 23 alineatul (2) litera (h) din RGPD] este recunoscut de articolul 7 din Circulara nr. 420 emisă de președintele Organizației Europene de Brevete.

29. În mod similar articolului 23 din RGPD, articolul 25 din Normele privind protecția datelor prevede că anumite dispoziții legale din cadrul juridic al Organizației Europene de Brevete pot restricționa aplicarea drepturilor prevăzute la articolele 18-25 din Normele privind protecția datelor și prevede conținutul minim pe care trebuie să-l includă măsurile care prevăd restricțiile. Acest conținut minim îl reflectă pe cel impus de RGPD. În plus, orice evaluare a necesității restricționării trebuie documentată corespunzător.

30. Până în prezent, Organizația Europeană de Brevete a implementat această dispoziție prin Circulara nr. 420, care clarifică ce drepturi pot fi restricționate și pentru ce obiective. De asemenea, se precizează că restricția va fi temporară și că îi revine operatorului sarcina de a stabili dacă, în funcție de circumstanțele relevante, se aplică restricția. În acest sens, operatorul va efectua, de la caz la caz, o evaluare a necesității și a proporționalității pentru fiecare caz în parte, care trebuie documentată și comunicată responsabilului cu protecția datelor al Organizației Europene de Brevete. RPD-ul are competența de a solicita revizuirea unei restricții, iar operatorul trebuie să informeze în scris cu privire la rezultatul revizuirii.

31. CEPD constată cu satisfacție că, în conformitate cu articolul 25 alineatele (2) și (4) din Normele privind protecția datelor și cu articolul 7 din Circulara nr. 420, persoanele vizate trebuie informate cu privire la restricții, cu excepția cazului în care acest lucru ar anula efectul restricției (în conformitate cu articolul 23 din RGPD și cu articolul 25 din RPDUE), precum și cu privire la dreptul lor de a consulta RPD-ul în vederea contestării restricțiilor și a drepturilor lor în temeiul articolelor 49 și 50 din Normele privind protecția datelor [articolul 25 alineatul (3) litera (b) din Normele privind protecția datelor]. În acest context, CEPD apreciază că informațiile privind restricțiile drepturilor persoanelor vizate sunt disponibile pe site-ul Organizației Europene de Brevete, în conformitate cu articolul 7 din Circulara nr. 420.

32. În plus, CEPD observă că există o serie de limitări ale drepturilor persoanelor vizate din cauza sarcinilor Organizației Europene de Brevete. De exemplu, Organizația Europeană de Brevete are obligația de a menține Registrul european de brevete, în care sunt publicate anumite date cu caracter personal definite legal. De asemenea, drepturile la rectificare și ștergere sunt limitate: Organizația Europeană de Brevete nu poate asigura rectificarea informațiilor - inclusiv a datelor cu caracter personal - conținute în documentele utilizate în procedura de acordare a brevetelor (cum este cazul documentelor aparținând procedurilor oficiale și judiciare, cum ar fi cererea de brevetare sau declarația de răspuns), iar Organizația Europeană de Brevete trebuie să respecte perioade de păstrare și cerințe de publicare specifice pentru anumite documente utilizate în procedura de acordare a brevetelor [articolul 129 litera (a) din Convenția privind brevetul european].

33. CEPD observă că restricțiile drepturilor persoanelor vizate prevăzute de Organizația Europeană de Brevete se limitează la ceea ce este strict necesar și proporțional pentru a asigura funcționarea corectă a procedurii de acordare a brevetelor, respectând astfel esența drepturilor și libertăților fundamentale ale persoanelor vizate, precum și cerințele de necesitate și proporționalitate prevăzute în Carta drepturilor fundamentale a Uniunii Europene (carta) și în Convenția pentru apărarea drepturilor omului și a libertăților fundamentale.

2.3 Restricții privind transferurile ulterioare

34. Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD precizează că nivelul de protecție a persoanelor fizice ale căror date cu caracter personal sunt transferate în temeiul unei decizii privind caracterul adecvat al nivelului de protecție nu trebuie afectat de transferul ulterior și, prin urmare, orice transfer ulterior „ar trebui permis doar atunci când destinatarul ulterior (adică destinatarul transferului ulterior) este supus tot unor norme (inclusiv normelor contractuale) care acordă un nivel adecvat de protecție și respectă instrucțiunile relevante atunci când prelucrează date în numele operatorului de date”[15]. Deși Normele privind protecția datelor fac distincție între așa-numitele „transmiteri de date cu caracter personal” și „transferuri de date cu caracter personal” și prevăd norme diferite pentru aceste două categorii de transferuri[16], CEPD subliniază că cerința de a nu afecta nivelul de protecție se aplică tuturor transferurilor ulterioare de date cu caracter personal transferate din UE, indiferent de terminologia utilizată.

35. CEPD observă că norme similare cu cele din capitolul V din RGPD se aplică „transferurilor de date cu caracter personal” [astfel cum sunt definite la articolul 3 litera (t) din Normele privind protecția datelor] pentru a se asigura că nivelul de protecție garantat de Normele privind protecția datelor nu este afectat (articolele 9 și 10 din Normele privind protecția datelor).

36. CEPD salută această aliniere strânsă cu capitolul V din RGPD și observă cu satisfacție că ghidul referitor la transfer al responsabilului cu protecția datelor face trimitere la orientările CEPD și la evoluțiile din cadrul Uniunii[17].

37. Având în vedere cele de mai sus, CEPD și-a concentrat evaluarea asupra normelor aplicabile celeilalte categorii de transferuri în temeiul Normelor privind protecția datelor, și anume „transmiterile de date cu caracter personal”.

2.3.1 Transmiterile de date cu caracter personal

38. În conformitate cu articolul 3 litera (s) din Normele privind protecția datelor, „transmiterea datelor cu caracter personal” se referă la „dezvăluirea, diseminarea sau punerea la dispoziție în alt mod, inclusiv prin acordarea accesului, a datelor cu caracter personal către o parte din cadrul Organizației Europene de Brevete sau către un oficiu național pentru proprietate industrială sau altă autoritate publică dintr-un stat contractant la Convenția brevetului european, în condițiile prevăzute la articolul 8”.

[15] Grupul de lucru „Articolul 29”, WP 254 rev. 01, adoptat la 28 noiembrie 2017 și revizuit și adoptat ultima dată la 6 februarie 2018, aprobat de CEPD, capitolul 3, A.9.
[16] Vezi considerentele 62-72 din proiectul de decizie.
[17] EPO transmission and transfer of personal data (Transmiterea și transferul datelor cu caracter personal de către Organizația Europeană de Brevete), notă explicativă, versiunea din ianuarie 2024, partea 3.2 (p. 9).

39. Articolul 8 alineatul (1) din Normele privind protecția datelor prevede că transmiterea datelor cu caracter personal către o autoritate publică a unui stat contractant al Organizației Europene de Brevete poate avea loc dacă datele sunt necesare pentru îndeplinirea sarcinilor respectivei autorități publice și dacă transmiterea este compatibilă cu sarcinile și funcționarea Organizației Europene de Brevete[18]. Articolul 8 alineatul (2) din Normele privind protecția datelor permite transmiterea datelor cu caracter personal către un oficiu național de proprietate industrială dintr-un stat contractant al Organizației Europene de Brevete, dacă datele sunt necesare pentru îndeplinirea sarcinilor care țin de competența destinatarului și dacă exercitarea autorității sale oficiale și prelucrarea sunt necesare pentru îndeplinirea sarcinilor în exercitarea activităților oficiale ale Organizației Europene de Brevete sau în exercitarea legitimă a autorității oficiale conferite operatorului, care include prelucrarea necesară pentru gestionarea și funcționarea Organizației Europene de Brevete. Astfel de transmiteri au loc în contextul procedurii de acordare a brevetelor prevăzute de CBE și de Tratatul de cooperare în domeniul brevetelor[19].

40. Destinatarii vor furniza dovezi că este necesar ca datele să fie transmise într-un scop specific care decurge din obligațiile Organizației Europene de Brevete de cooperare cu statul contractant, iar operatorul – în cazul în care interesele legitime ale persoanei vizate ar putea fi afectate – va stabili dacă transmiterea datelor în acel scop specific este proporțională, după ce a evaluat în mod demonstrabil interesele concurente [articolul 8 alineatele (3) și (4) din Normele privind protecția datelor].

41. Pentru a oferi garanții adecvate ca instrumente pentru transmiteri, ar trebui introduse dispoziții specifice privind protecția datelor în instrumentele executorii, cum ar fi memorandumurile de înțelegere sau acordurile administrative[20]. Responsabilul cu protecția datelor al Organizației Europene de Brevete a întocmit clauze standard de protecție a datelor pentru memorandumurile de înțelegere, care prevăd, printre altele, principii de protecție a datelor, inclusiv, de exemplu, limitări legate de scop, drepturile persoanelor vizate, precum și supravegherea independentă și mecanisme adecvate de aplicare[21]. CEPD recunoaște existența unor astfel de garanții, dar observă că cerința de a nu afecta nivelul de protecție nu este menționată în mod specific în legătură cu transmiterile, nici în articolul 8 din Normele privind protecția datelor, nici în nota explicativă a Organizației Europene de Brevete privind transmiterea și transferul datelor cu caracter personal, nici în proiectul de decizie privind caracterul adecvat al nivelului de protecție. CEPD observă că, în schimb, această cerință este menționată în mod expres în contextul transferurilor[22] și solicită Comisiei să clarifice acest aspect.

[18] Vezi considerentul 63 din proiectul de decizie; acest lucru ar putea avea ca scop cooperarea prin procese de consultare; detașarea și mobilizarea de experți; furnizarea de informații privind personalul Organizației Europene de Brevete în scopul stabilirii prestațiilor sociale, a obligațiilor fiscale etc.

[19] Vezi considerentul 62, nota de subsol 165 din proiectul de decizie și JO Organizația Europeană de Brevete 2021, A98 – Decizia președintelui Oficiului European de Brevete din 13 decembrie 2021 privind prelucrarea datelor cu caracter personal în cadrul procedurilor de acordare a brevetelor și al procedurilor conexe.

[20] EPO transmission and transfer of personal data (Transmiterea și transferul datelor cu caracter personal de către Organizația Europeană de Brevete), notă explicativă, versiunea din ianuarie 2024, p. 6.

[21] Prezentare generală a cerințelor clauzei standard de protecție a datelor a Organizației Europene de Brevete pentru memorandumurile de înțelegere, versiunea din iunie 2024.

[22] Vezi considerentul 67 din proiectul de decizie.

42. În plus, CEPD a înțeles din explicațiile suplimentare oferite de Comisie că cerința privind garanțiile adecvate ca instrumente pentru transmiteri nu se aplică în cazul în care destinatarul este un oficiu național de proprietate industrială. În consecință, CEPD nu are o imagine clară asupra garanțiilor în materie de protecție a datelor care se aplică atunci când datele cu caracter personal sunt transmise în contextul procedurii de acordare a brevetelor. Prin urmare, CEPD invită Comisia să clarifice și acest aspect.

2.4 Mecanisme procedurale și de punere în aplicare

43. Conform Criteriilor de referință privind caracterul adecvat al nivelului de protecție[23] și jurisprudenței relevante a CJUE[24], un sistem de protecție a datelor în esență echivalent cu modelul Uniunii Europene trebuie să prevadă: (i) o autoritate independentă, care ar trebui să supravegheze și să aplice legile privind protecția datelor, cu competența de a investiga și de a lua măsuri fără influențe externe. Sistemele de protecție a datelor trebuie să asigure (ii) că operatorii și persoanele împuternicite de operatori sunt responsabili și își cunosc responsabilitățile, iar persoanele vizate sunt informate cu privire la drepturile lor. Ar trebui să existe sancțiuni și procese de verificare eficiente pentru a asigura respectarea normelor; (iii) operatorii și persoanele împuternicite de operatori demonstrează conformitatea, prin măsuri precum evaluări ale impactului asupra protecției datelor, evidențe ale activităților de prelucrare și numirea unor responsabili cu protecția datelor. În plus, (iv) sistemul de protecție a datelor trebuie să ofere sprijin și ajutor persoanelor vizate în exercitarea drepturilor lor și mecanisme de recurs adecvate.

44. În ceea ce privește principiul responsabilității care acoperă punctele (ii) și (iii) din paragraful anterior, CEPD face referire la secțiunea 2.1.2 de mai sus.

45. În secțiunile următoare, CEPD și-a concentrat evaluarea asupra existenței unei autorități independente și a unor mecanisme adecvate de recurs.

1.

2.

2.1

2.2

2.3

2.4

2.4.1 Responsabilul cu protecția datelor și Comitetul pentru protecția datelor

46. Sistemul prezentat de Organizația Europeană de Brevete stabilește două organisme distincte responsabile cu supravegherea respectării normelor privind protecția datelor: responsabilul cu protecția datelor și Comitetul pentru protecția datelor (articolul 32A din Regulamentul de funcționare).

[23] Grupul de lucru „Articolul 29”, WP 254 rev. 01, adoptat la 28 noiembrie 2017 și revizuit și adoptat ultima dată la 6 februarie 2018, aprobat de CEPD, capitolul 3, C.
[24] CJUE, 6 octombrie 2015, Hotărârea în cauza C-362/14, Maximillian Schrems/Data Protection Commissioner („Schrems”).

47. Responsabilul cu protecția datelor al Organizației Europene de Brevete, pe lângă îndeplinirea rolului tradițional de RPD în temeiul RGPD, deține și competențe de investigare în conformitate cu articolul 43 din Normele privind protecția datelor.

48. Rolul Comitetului pentru protecția datelor este de a asigura supravegherea independentă, eficientă și imparțială a normelor privind protecția datelor. Persoanele vizate au dreptul de a depune plângere la Comitetul pentru protecția datelor dacă nu sunt de acord cu o decizie sau cu respingerea implicită a unei cereri de reexaminare de către un operator delegat (articolul 50 din Normele privind protecția datelor).

49. Deși această structură dual, justificată de natura Organizației Europene de Brevete, nu este în mod inerent îngrijorătoare sau problematică, este esențial ca ambele organisme să funcționeze în deplină independență pentru a asigura o supraveghere și o aplicare eficace și să dispună de toate competențele necesare pentru a-și îndeplini sarcinile.

50. În acest sens, CEPD și-a concentrat evaluarea asupra independenței efective a acestor organisme de supraveghere și asupra competențelor lor. În ceea ce privește independența, CEPD salută nu numai formularea care susține acest principiu în articolele relevante, ci și garanțiile suplimentare existente.

51. În acest cadru, CEPD a examinat normele care reglementează numirea, revocarea și demiterea responsabilului cu protecția datelor și a Comitetului pentru protecția datelor, în special cerința ca președintele să consulte Comitetul pentru protecția datelor înainte de orice propunere de revocare sau demitere a RPD-ului.

52. CEPD consideră că această consultare prealabilă reprezintă o potențială garanție a independenței RPD-ului, însă natura și implicațiile unei astfel de consultări rămân neclare. Prin urmare, CEPD invită Comisia să clarifice mai bine acest aspect și să ia în considerare monitorizarea, în cadrul revizuirilor viitoare, a faptului că, în practică, RPD-ul nu este demis sau sancționat de operator pentru îndeplinirea atribuțiilor sale.

53. CEPD observă că, în conformitate cu articolul 47 din Normele privind protecția datelor, CPD are funcție de supraveghere și consultativă, întrucât oferă consultanță operatorului și operatorilor delegați în legătură cu aplicarea articolelor 38 și 39 din Normele privind protecția datelor, oferă consultanță cu privire la demiterea RPD-ului în temeiul articolului 48 alineatul (2) din Normele privind protecția datelor și emite un aviz cu privire la utilizarea mecanismului de recurs în temeiul articolului 50.

54. În ceea ce privește numirea membrilor CPD, CEPD observă că, în conformitate cu articolul 48 alineatul (1) din Normele privind protecția datelor, Comitetul pentru protecția datelor este compus din trei experți externi în domeniul protecției datelor numiți de președintele Oficiului, și anume un președinte și alți doi membri, dintre care unul îndeplinește funcția de vicepreședinte. În conformitate cu articolul 48 alineatul (2) din Normele privind protecția datelor, președintele, ceilalți doi membri și membrii supleanți ai Comitetului pentru protecția datelor trebuie să dețină calificările necesare pentru numirea în funcții judiciare sau să fie profesioniști în domeniul protecției datelor, având experiență și cunoștințe de specialitate dovedite în acest domeniu.

55. CEPD apreciază că normele de selecție a membrilor organismului de supraveghere impun cunoștințe de specialitate în domeniul protecției datelor și încurajează Comisia să monitorizeze dacă membrii Comitetului pentru protecția datelor selectați pe baza calificărilor lor au nivelul necesar de cunoștințe de specialitate în domeniul protecției datelor, având în vedere importanța sa pentru funcția de supraveghere.

2.4.2 Competențe de investigare și corective

56. În acest context, CJUE a clarificat că competențele autorităților de supraveghere constituie mijloace necesare pentru îndeplinirea atribuțiilor lor și că acestea ar trebui să dispună, în special, de competențe de investigare, cum ar fi competența de a aduna toate informațiile necesare pentru îndeplinirea atribuțiilor lor de supraveghere, de competențe efective de intervenție, cum ar fi cea de a impune o interdicție temporară sau definitivă privind prelucrarea datelor, și de competența de a iniția proceduri judiciare[25].

57. În conformitate cu articolul 43 alineatul (1) litera (d), RPD-ul poate efectua audituri de protecție a datelor și investigații (efectuate sub formă de inspecții privind protecția datelor sau anchete *ad hoc*)[26]. Conform notei privind „Supravegherea protecției datelor”[27], care detaliază articolul 43 din Normele privind protecția datelor, RPD-ul, în consultare cu CPD, pregătește un plan anual de audit privind protecția datelor (planul) și îl prezintă președintelui Organizației Europene de Brevete spre aprobare. Planul aprobat este prezentat Comitetului pentru protecția datelor spre informare. CPD poate oricând să formuleze sugestii cu privire la domeniile în care Oficiul ar trebui să efectueze un audit privind protecția datelor.

58. În conformitate cu articolul 43 alineatul (1) litera (i) din Normele privind protecția datelor, RPD-ul trebuie să răspundă la solicitările Comitetului pentru protecția datelor și să coopereze și să se consulte cu CPD la cererea acestuia sau din proprie inițiativă. În conformitate cu articolul 43 alineatul (1) litera (j) din Normele privind protecția datelor, RPD-ul trebuie să faciliteze cooperarea între Comitetul pentru protecția datelor și Oficiu în ceea ce privește, printre altele, investigațiile privind protecția datelor, tratarea plângerilor, evaluările impactului asupra protecției datelor și consultările prealabile. RPD-ul trebuie, de asemenea, să transmită Comitetului pentru protecția datelor informații despre noile măsuri administrative și normele interne referitoare la prelucrarea datelor cu caracter personal.

59. RPD-ul completează un raport privind investigațiile și auditurile efectuate și, dacă identifică nerespectarea normelor de protecție a datelor, raportul va include constatările, concluziile și recomandările sale (inclusiv măsurile de remediere).

60. În special, în conformitate cu nota privind „Supravegherea protecției datelor”, recomandările pot include „măsuri preventive, de atenuare sau corective” pentru operatorul de date în caz de nereguli sau de nerespectare a normelor. RPD-ul poate recomanda aducerea operațiunilor de prelucrare în conformitate cu Normele privind protecția datelor; respectarea cererilor persoanelor vizate de a-și exercita drepturile în temeiul Normelor privind protecția datelor; comunicarea unei încălcări a datelor cu caracter personal către persoana (persoanele) vizată (vizate); suspendarea unei anumite operațiuni de prelucrare a datelor; sau suspendarea fluxului de date către anumiți destinatari[28].

---

[25] CJUE, 6 octombrie 2015, Hotărârea în cauza C-362/14, Maximillian Schrems/Data Protection Commissioner („Schrems”), punctul 43.

[26] Competențele de investigare ale RPD-ului sunt detaliate în documentul „Data Protection Oversight – How the Data Protection Office conducts DP Audits and DP Inspections” (Supravegherea protecției datelor – Desfășurarea auditurilor și a controalelor cu privire la protecția datelor de către serviciul responsabil cu protecția datelor), disponibil pe site-ul Organizației Europene de Brevete la următorul link https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-data-protection-oversight-mechanism.pdf.

[27] „Data Protection Oversight – How the Data Protection Office conducts DP Audits and DP Inspections” (Supravegherea protecția datelor – Desfășurarea auditurilor și a controalelor cu privire la protecția datelor de către serviciul responsabil cu protecția datelor”), disponibil pe site-ul Organizației Europene de Brevete la următorul link https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-data-protection-oversight-mechanism.pdf.

[28] *Ibid*.

61. În conformitate cu nota privind „Supravegherea protecției datelor” și cu Decizia președintelui Oficiului din 12.7.2024[29], concluziile și recomandările pot deveni obligatorii (sub rezerva validării de către Comitet) și trebuie puse în aplicare de către operator. Conform notei privind „Supravegherea protecției datelor”, care detaliază regulile prevăzute la articolul 43 alineatul (1) literele (i) și (j) din Normele privind protecția datelor, CPD are competența de a formula observații cu privire la concluzii și recomandări și, de asemenea, de a solicita modificări, care vor fi puse în aplicare de RPD. În plus, RPD-ul are autoritatea de a iniția inspecții de monitorizare ulterioară sau de a extinde domeniul de aplicare al inspecțiilor privind protecția datelor și de a recomanda demararea unei anchete administrative pentru a stabili dacă sunt necesare măsuri disciplinare sau de altă natură.

62. Având în vedere legătura strânsă dintre RPD și CPD, precum și importanța competențelor de investigare, de auditare și corective, CEPD recomandă Comisiei să clarifice în continuare interacțiunea dintre acestea, în special în ceea ce privește exercitarea competențelor de investigare, de auditare și corective, precum și să clarifice rolul RPD-ului în tratarea cererilor persoanelor vizate [articolul 43 alineatul (1) litera (k) din Normele privind protecția datelor] și rolul său, dacă este cazul, în procedura de depunere a plângerilor la CPD, în conformitate cu articolul 50 din Normele privind protecția datelor. În special, CEPD invită Comisia să monitorizeze dacă se face o distincție clară în practică între momentele în care RPD-ul acționează în nume propriu (îndeplinindu-și rolul și funcția de RPD) și momentele în care acționează în numele CPD-ului pentru a-l sprijini în îndeplinirea funcțiilor sale de supraveghere. Acest lucru ar oferi o claritate suplimentară cu privire la structura de supraveghere și la rolul RPD-ului și al CPD-ului.

2.4.3 Procedura de depunere a plângerilor la Comitetul pentru protecția datelor

63. CEPD observă că persoanele vizate au dreptul de a depune plângere la Comitetul pentru protecția datelor, care o tratează în conformitate cu procedura prevăzută la articolul 50 din Normele privind protecția datelor și cu regulamentul de procedură prevăzut în anexa 1 la Normele privind protecția datelor.

64. În special, după examinarea plângerii, CPD emite un aviz motivat către operator, în care poate recomanda acordarea de despăgubiri pentru prejudicii materiale sau morale.

65. În conformitate cu articolul 50 alineatul (4) din Normele privind protecția datelor, avizele motivate ale CPD-ului (denumite în continuare „avize”) nu sunt obligatorii pentru operatorul de date, care poate alege să nu le respecte. În acest caz, operatorul trebuie să furnizeze o explicație scrisă și i se solicită, de asemenea, să informeze persoana vizată, operatorul delegat și, după caz, persoana împuternicită de operator, RPD-ul și CPD-ul cu privire la decizia sa finală și la concluziile CPD-ului. Decizia (constituită din avizul motivat al CPD-ului și decizia finală a operatorului) poate fi contestată de persoana vizată, solicitând președintelui Oficiului să inițieze procedura de arbitraj prevăzută la articolul 52 din Normele privind protecția datelor sau prin intermediul Tribunalului Administrativ al Organizației Internaționale a Muncii.

66. În conformitate cu orientările CEPD, Criteriile de referință privind caracterul adecvat al nivelului de protecție și jurisprudența CJUE, organismul de supraveghere va avea competențe obligatorii, deoarece este un factor esențial în asigurarea eficacității mecanismului de supraveghere.

[29] Decizia Președintelui Oficiului privind forța executorie a recomandărilor responsabilului cu protecția datelor aprobate de Comitetul pentru protecția datelor în cadrul auditurilor și controalelor privind protecția datelor. Concluziile sunt disponibile la următorul link https://link.epo.org/web/office/data-protection-and-privacy/en-decision-of-the-president-on-enforceability-of-dpo-conclusions-and-recommendations.pdf.

67. CEPD observă că avizele Comitetului pentru protecția datelor emise în contextul tratării plângerilor rămân neobligatorii. Deși concluziile și recomandările RPD-ului – în urma investigațiilor și auditurilor, care ar fi putut fi inițiate la cererea CPD-ului – pot deveni obligatorii după aprobarea de către CPD, acestea nu par să se aplice cazurilor inițiate în temeiul articolului 50 din Normele privind protecția datelor, adică plângerilor persoanelor vizate.

68. Având în vedere cele de mai sus, CEPD invită Comisia să verifice și să se asigure că competențele CPD-ului sunt obligatorii în contextul tratării plângerilor în temeiul articolului 50 din Normele privind protecția datelor și să evalueze dacă pot fi prevăzute garanții suplimentare în acest sens.

69. Cu toate acestea, CEPD salută faptul că deciziile operatorului în temeiul articolului 50 alineatul (6) din Normele privind protecția datelor pot fi contestate, deoarece acest lucru oferă persoanelor vizate mecanismele de recurs necesare și permite punerea în aplicare a deciziei organismului de supraveghere.

70. De asemenea, CEPD salută faptul că și CPD-ul poate recomanda acordarea de despăgubiri pentru prejudicii materiale sau morale [articolul 50 alineatul (3) din Normele privind protecția datelor].

2.4.4 Mecanisme de recurs și arbitraj

71. Conform Criteriilor de referință privind caracterul adecvat al nivelului de protecție, persoanelor vizate ar trebui să li se ofere căi de atac eficiente, inclusiv despăgubiri pentru prejudiciile rezultate din prelucrarea ilegală a datelor lor cu caracter personal. Acesta este un element esențial care trebuie să implice un sistem de judecată sau arbitraj independent, care să permită plata de despăgubiri și impunerea de sancțiuni, după caz.

72. CEPD observă că, în conformitate cu cadrul legal privind protecția datelor al Organizației Europene de Brevete, persoanele vizate au dreptul de a solicita revizuirea prelucrării datelor lor cu caracter personal în fața operatorilor delegați atunci când consideră că a avut loc o încălcare a normelor de protecție a datelor. Aceasta constituie o condiție prealabilă pentru depunerea unei plângeri la CPD în calitate de organism independent de supraveghere, în conformitate cu articolul 50 din Normele privind protecția datelor. Această cerință reprezintă o caracteristică nouă în comparație cu sistemul de protecție a datelor al UE, care însă nu afectează nivelul de protecție oferit de sistemul Organizației Europene de Brevete, deoarece nu afectează nici aplicabilitatea drepturilor persoanelor vizate, nici dreptul lor la despăgubiri.

73. În conformitate cu articolul 50 și articolul 52 alineatul (1) din Normele privind protecția datelor, dacă nu sunt mulțumite de decizia finală luată în urma procedurii prevăzute la articolul 50 din Normele privind protecția datelor, persoanele vizate pot introduce o cale de atac. Angajații Organizației Europene de Brevete pot contesta decizia la Tribunalul Administrativ al Organizației Internaționale a Muncii. Orice altă persoană vizată are la dispoziție trei luni pentru a depune cerere de arbitraj la președinte.

74. CEPD salută dispozițiile privind mecanismul de recurs. În ceea ce privește mecanismul de arbitraj, CEPD observă că este posibil să se prevadă mecanisme alternative de soluționare a litigiilor, atunci când mecanismele judiciare nu sunt disponibile, de exemplu, din cauza statutului operatorului ca organizație internațională. Aceste mecanisme alternative de soluționare a litigiilor trebuie să ofere persoanelor vizate garanții echivalente în esență cu cele prevăzute la articolul 47 din Cartă[30]. Prin urmare, prevederea unui mecanism alternativ nu prezintă în sine motive de îngrijorare sau probleme inerente[31], cu condiția ca arbitrajul (i) să garanteze o judecată independentă și imparțială, în conformitate cu principiile unui proces echitabil, (ii) să fie obligatoriu pentru operator (Organizația Europeană de Brevete)[32], să permită (iii) acordarea de despăgubiri și (iv) impunerea de sancțiuni, dacă este cazul.

75. În mod similar, Curtea Europeană a Drepturilor Omului a hotărât că se pot asigura căi de atac eficiente prin „mijloace alternative rezonabile", cum ar fi arbitrajul [33].

76. CEPD constată cu satisfacție că cadrul juridic al Organizației Europene de Brevete prevede (i) norme care să asigure independența arbitrului [articolul 52 alineatul (3) din Normele privind protecția datelor], (ii) caracterul obligatoriu al mecanismului de arbitraj [articolul 52 alineatul (1) din Normele privind protecția datelor], precum și (iii) dreptul la despăgubiri pentru prejudiciile suferite ca urmare a încălcării normelor privind protecția datelor [articolul 53 din Normele privind protecția datelor] și (iv) impunerea de sancțiuni, după caz (articolul 11 din Regulamentul de arbitraj al Curții Europene de Arbitraj[34]).

77. În plus, CEPD salută faptul că Organizația Europeană de Brevete suportă costurile arbitrajului , îndeplinind astfel cerința potrivit căreia căile de atac pentru asigurarea respectării drepturilor persoanelor vizate nu trebuie să implice costuri prohibitive[35].

[30] CJUE, 16 iulie 2020, Hotărârea în cauza C-311/18, Data Protection Commissioner/Facebook Ireland Limited și Maximillian Schrems („Schrems II"), punctele 96 și 186 și următoarele.
[31] Grupul de lucru „Articolul 29", Criteriile de referință privind caracterul adecvat al nivelului de protecție adoptate la 28 noiembrie 2017, revizuite și adoptate ultima dată la 6 februarie 2018; Orientările 2/2020 privind articolul 46 alineatul (2) litera (a) și articolul 46 alineatul (3) litera (b) din Regulamentul (UE) 2016/679 pentru transferurile de date cu caracter personal între autoritățile și organismele publice din SEE și din afara SEE, versiunea 2.0, adoptată la 15 decembrie 2020, punctele 53 și 75.
[32] CJUE, 6 octombrie 2015, Hotărârea în cauza C-362/14, Maximillian Schrems/Data Protection Commissioner („Schrems"), punctele 41 și 95; CJUE, 16 iulie 2020, Hotărârea în cauza C-311/18, Data Protection Commissioner/Facebook Ireland Ltd și Maximillian Schrems („Schrems II"), punctele 186, 187, 189, 195 și următoarele.
[33] CEDO, Secția a cincea, Hotărâre, Cererea nr. 415/07. Roland KLAUSECKER împotriva Germaniei, disponibilă la următorul link https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-151029%22.
[34] Regulamentul de arbitraj al Curții Europene de Arbitraj este disponibil la următorul link https://cour-europe-arbitrage.org/arbitration-rules/
[35] Grupul de lucru „Articolul 29", WP 254 rev. 01, adoptat la 28 noiembrie 2017 și revizuit și adoptat ultima dată la 6 februarie 2018, aprobat de CEPD, punctul 4.

3. ACCESAREA ȘI UTILIZAREA DE CĂTRE AUTORITĂȚILE PUBLICE A DATELOR CU CARACTER PERSONAL TRANSFERATE DIN UNIUNE CĂTRE ORGANIZAȚIA EUROPEANĂ DE BREVETE

78. CEPD subliniază, în primul rând, că evaluarea accesului autorităților publice la datele cu caracter personal transferate din Uniune și a utilizării lor de către acestea este, în cazul de față, distinctă de evaluarea corespunzătoare a nivelului de protecție oferit de o țară terță. În loc să evalueze legislația și practicile relevante ale țării terțe în materie de acces al autorităților publice, scenariul specific al unei decizii privind protecția adecvată a datelor cu caracter personal de către o organizație internațională necesită revizuirea normelor care determină modul în care organizația respectivă tratează cererile autorităților publice de acces la date cu caracter personal, inclusiv, în special, posibilitatea și normele de respingere a acestor cereri. Prin urmare, standardul în raport cu care se evaluează echivalența în esență diferă, în ceea ce privește accesul autorităților publice la date, de deciziile anterioare privind caracterul adecvat al nivelului de protecție.

79. Ca observație generală suplimentară, CEPD constată în continuare că, potrivit explicațiilor suplimentare furnizate de Comisie, Organizația Europeană de Brevete nu a primit încă nicio cerere de acces la date în scopul aplicării legii sau al securității naționale.

80. Faptul că, până în prezent, la Organizația Europeană de Brevete nu au fost depuse cereri în scopul aplicării legii sau al securității naționale înseamnă că normele aplicabile în astfel de cazuri nu au fost încă testate în practică în acest sens. Prin urmare, CEPD încurajează Comisia să monitorizeze dacă Organizația Europeană de Brevete va primi astfel de cereri în viitor și modul de punere în aplicare a normelor relevante în contextul specific. Comisia ar putea examina, în special, modul în care normele și standardele Organizației Europene de Brevete se aplică în cazul cererilor autorităților de aplicare a legii și ale serviciilor de informații, cum ar fi cerința de a furniza dovezi că este necesară transmiterea datelor într-un scop specific care decurge din obligația Organizației Europene de Brevete de a coopera [articolul 8 alineatul (3) din Normele privind protecția datelor]. Astfel de dovezi vor sta, la rândul lor, la baza evaluării de către Organizația Europeană de Brevete a necesității și proporționalității unei transmiteri [articolul 8 alineatul (4) din Normele privind protecția datelor][36].

3.1 Prelucrarea de către Organizația Europeană de Brevete a cererilor de acces la date cu caracter personal din partea autorităților publice

81. Proiectul de decizie precizează că cadrul juridic în temeiul căruia Organizația Europeană de Brevete evaluează și răspunde la cererile autorităților publice privind datele cu caracter personal decurge din PPI, din cerințele Normelor privind protecția datelor referitoare la transmiterea și transferul datelor cu caracter personal și din dreptul internațional public[37]. Deși acest cadru se aplică în general cererilor provenite atât din statele contractante, cât și din statele necontractante, dispozițiile specifice stabilesc un regim diferit pentru cererile emise de autoritățile publice ale statelor contractante, pe de o parte, și ale statelor necontractante, pe de altă parte.

[36] În ceea ce privește cadrul juridic al transmiterilor, vezi și punctele 56 și 57 din prezentul aviz.
[37] Vezi considerentul 96 din proiectul de decizie.

82. În ceea ce privește statele contractante, imunitățile Organizației Europene de Brevete prevăzute în PPI (vezi punctul 14) sunt completate de o obligație de cooperare. Articolul 20 alineatul (1) din PPI prevede că Organizația Europeană de Brevete „va coopera în permanență cu autoritățile competente ale statelor contractante pentru a facilita buna administrare a justiției, pentru a asigura respectarea reglementărilor în domeniul polițienesc și a reglementărilor privind sănătatea publică, inspecția muncii sau alte reglementări naționale similare și pentru a preveni orice utilizare abuzivă a privilegiilor, a imunităților și a facilităților prevăzute în prezentul protocol”[38]. În acest scop și în conformitate cu articolul 3 alineatul (1) litera (a) din PPI, Organizația Europeană de Brevete poate renunța la imunitatea sa de jurisdicție și de executare pentru a răspunde cererilor de acces ale autorităților publice. CEPD constată în mod corespunzător că pare într-adevăr inevitabil să se prevadă mecanisme de cooperare cu autoritățile publice din statele contractante, care, în anumite cazuri, pot chiar servi intereselor persoanei vizate, de exemplu în ceea ce privește prestațiile sociale și aspectele legate de asigurări ale personalului Organizației Europene de Brevete. Cu toate acestea, articolul 20 alineatul (1) din PPI ridică problema, în special în ceea ce privește cererile de acces în scopul aplicării legii și al securității naționale, a modului în care obligația de cooperare se raportează la conceptul de imunitate sau interacționează cu acesta. Comisia a indicat că normele Organizației Europene de Brevete privind cooperarea ar trebui să fie înțelese ca făcând parte din principiul general mai larg al imunității și, prin urmare, Organizația Europeană de Brevete ar fi în măsură să respingă cererile în scopurile menționate mai sus, indiferent de articolul 20 alineatul (1) din PPI. CEPD invită Comisia să clarifice în continuare acest aspect în decizie.

83. Decizia privind o cerere de cooperare revine președintelui Oficiului, care, astfel cum se indică în proiectul de decizie, exercită o putere discreționară în acest sens[39]. Deși proiectul de decizie se referă la articolul 3 alineatul (1) litera (a) din PPI ca temei juridic pentru renunțarea la imunitatea organizației, acesta nu identifică în mod clar o dispoziție care să confere președintelui puterea discreționară în cauză și să stabilească criteriile care orientează exercitarea acestei puteri discreționare atunci când se decide cu privire la o cerere de cooperare. CEPD observă că, în temeiul articolului 19 alineatul (2) din PPI, președintele „are obligația de a renunța la imunitate în cazul în care consideră că aceasta împiedică desfășurarea normală a justiției și că este posibil să se renunțe la această imunitate fără a prejudicia interesele organizației”. Această cerință ridică întrebări suplimentare cu privire la domeniul de aplicare a puterii discreționare a președintelui. În continuarea paragrafului anterior, CEPD invită Comisia să clarifice aceste aspecte în decizie.

84. Dacă Organizația Europeană de Brevete decide să dea curs unei cereri de acces din partea unui stat contractant în conformitate cu articolul 20 alineatul (1) din PPI, se aplică cerințele din Normele privind protecția datelor referitoare la transmiteri (vezi punctul 38 și următoarele)[40]. Aceste norme se aplică tuturor statelor contractante, indiferent dacă statul contractant este un stat membru al SEE sau este considerat țară terță din perspectiva legislației UE privind protecția datelor. Cu toate acestea, normele privind transmiterile, spre deosebire de regimul aplicabil transferurilor către autorități publice din afara statelor contractante ale Organizației Europene de Brevete, nu impun în mod explicit asigurarea unui nivel adecvat de protecție a datelor transferate în țara destinatară[41]. În acest sens, CEPD dorește să reamintească Orientările sale privind articolul 48 din RGPD[42], în care se precizează că „în cazul în

[38] Conform informațiilor suplimentare furnizate de Comisie, Organizația Europeană de Brevete nu a exercitat, până în prezent, competența conferită de articolul 20 alineatul (2) și articolul 25 din PPI de a încheia acorduri complementare cu unul sau mai multe state contractante în scopul aplicării legii sau al securității naționale.
[39] Vezi considerentul 97 din proiectul de decizie.
[40] *Ibid*.
[41] Vezi considerentele 63-65 din proiectul de decizie și articolul 8 din Normele privind protecția datelor.
[42] Orientările CEPD 02/2024 privind articolul 48 din RGPD, adoptate la 2 decembrie 2024.

care datele prelucrate în UE sunt transferate sau divulgate ca răspuns la o cerere din partea unei autorități dintr-o țară terță, o astfel de divulgare face obiectul RGPD și constituie un transfer în sensul capitolului V. Aceasta înseamnă că, la fel ca în cazul oricărui transfer care face obiectul RGPD, trebuie să existe un temei juridic pentru prelucrare la articolul 6 și un motiv de transfer în capitolul V".[43] În acest sens, CEPD își reafirmă solicitarea de clarificare exprimată la punctul 41 de mai sus și invită Comisia să clarifice ce garanții se aplică și în ceea ce privește transmiterile bazate pe cereri de acces din partea autorităților publice, în special cererile în scopul aplicării legii și al securității naționale. Ar trebui să se asigure că cerințele din capitolul V din RGPD, în măsura necesară pentru a stabili echivalența esențială, sunt îndeplinite în mod suficient, inclusiv în cazul în care conceptul de țări terțe din legislația UE privind protecția datelor și cadrul juridic al Organizației Europene de Brevete nu coincid pe deplin[44].

85. Deși CEPD recunoaște că nota explicativă a Organizației Europene de Brevete privind transmiterea și transferul datelor cu caracter personal prevede că „pentru a oferi garanții adecvate ca instrumente pentru transmiteri, ar trebui introduse dispoziții specifice privind protecția datelor în instrumente executorii, cum ar fi memorandumuri de înțelegere sau acorduri administrative[45]", în practică poate fi irealizabil să se pună în aplicare astfel de instrumente în relația cu autoritățile de aplicare a legii și serviciile naționale de securitate. CEPD consideră că transmiterea datelor cu caracter personal către state contractante care nu sunt membre ale SEE, în special în scopul aplicării legii și al securității naționale, ar necesita, prin urmare, o atenție specială din partea Comisiei.

86. Deoarece nu există niciun instrument juridic care să reglementeze în mod specific prelucrarea de către Organizația Europeană de Brevete a cererilor adresate de autoritățile publice ale statelor necontractante, se aplică normele generale privind transferurile în temeiul Normelor privind protecția datelor, care sunt foarte asemănătoare cu cele din capitolul V din RGPD (vezi punctele 35 și 36).

3.2 Restricționarea drepturilor persoanelor vizate

87. Articolul 25 din Normele privind protecția datelor prevede că dispozițiile juridice specifice din cadrul juridic al Organizației Europene de Brevete pot, în condiții care reflectă îndeaproape cerințele articolului 23 din RGPD, să restricționeze aplicarea drepturilor persoanelor vizate (vezi punctul 33 și următoarele). În contextul accesului autorităților publice, CEPD observă că restricția prevăzută în Circulara nr. 420 litera (h) poate permite o interpretare extinsă, întrucât se referă în sens larg la scenarii de „furnizare sau primire de asistență către sau de la autoritățile publice competente, inclusiv din partea statelor contractante ale Organizației Europene de Brevete și a organizațiilor internaționale". Deși recunoaște că domeniul de aplicare al acestei dispoziții este limitat la personalul Organizației Europene de Brevete, CEPD invită Comisia să monitorizeze aplicarea sa practică.

[43] *Ibid*., punctul 9.

[44] Deși CEPD recunoaște că toate statele contractante sunt părți la CEDO și la Convenția 108, CEPD reamintește că ratificarea acestor instrumente nu poate asigura, în sine, un nivel de protecție în esență echivalent, deoarece acest lucru va depinde, în special, de punerea lor în aplicare specifică în fiecare țară.

[45] EPO transmission and transfer of personal data (Transmiterea și transferul datelor cu caracter personal de către Organizația Europeană de Brevete), notă explicativă, versiunea din ianuarie 2024, p. 6.

4. PUNEREA ÎN APLICARE ȘI MONITORIZAREA PROIECTULUI DE DECIZIE

88. În ceea ce privește monitorizarea și revizuirea deciziei privind caracterul adecvat al nivelului de protecție, CEPD observă că, în conformitate cu jurisprudența CJUE, „având în vedere că nivelul de protecție asigurat de o țară terță sau de o organizație internațională este susceptibil să se modifice, revine Comisiei, după adoptarea unei decizii privind caracterul adecvat al protecției în temeiul articolului 45 din RGPD, sarcina de a verifica în mod periodic dacă constatarea referitoare la nivelul de protecție adecvat asigurat de țara terță sau de organizația internațională în cauză este în continuare justificată în fapt și în drept. O astfel de verificare se impune, în orice caz, atunci când există indicii care dau naștere unei îndoieli în această privință”[46].

89. CEPD consideră că funcția de supraveghere – și, în special, exercitarea competențelor de investigare și corective –, precum și accesul autorităților publice la datele transferate din UE către Organizația Europeană de Brevete vor merita o atenție specială în cadrul următoarelor revizuiri periodice. De asemenea, Comisia ar trebui să acorde o atenție sporită, în cadrul monitorizării deciziei privind caracterul adecvat al nivelului de protecție, evoluției normelor care completează Normele privind protecția datelor, cum ar fi *Decizia președintelui Oficiului European de Brevete din 12.7.2024 privind aplicabilitatea recomandărilor responsabilului cu protecția datelor aprobate de Comitetul pentru protecția datelor în cadrul auditurilor și inspecțiilor privind protecția datelor, Supravegherea protecției datelor – Desfășurarea auditurilor și a controalelor cu privire la protecția datelor de către serviciul responsabil cu protecția datelor* și *Transmiterea și transferul datelor cu caracter personal de către Organizația Europeană de Brevete, notă explicativă*, versiunea din ianuarie 2024.

90. CEPD observă că revizuirea constatării caracterului adecvat al nivelului de protecție va avea loc cel puțin o dată la patru ani, în conformitate cu articolul 45 alineatul (3) din RGPD.

91. În ceea ce privește implicarea practică a CEPD și a reprezentanților săi în pregătirea și desfășurarea viitoarelor revizuiri periodice, CEPD reiterează că orice documentație relevantă, inclusiv corespondența, ar trebui comunicată în scris CEPD cu suficient timp înainte de revizuiri.

92. CEPD salută faptul că proiectul de decizie prevede participarea CEPD la reuniunea organizată între Comisie și Organizația Europeană de Brevete și dedicată revizuirii funcționării deciziei privind caracterul adecvat al nivelului de protecție.

Pentru Comitetul european pentru protecția datelor

Președinta

(Anu Talus)

[46] CJUE, 6 octombrie 2015, Hotărârea în cauza C-362/14, Maximillian Schrems împotriva Data Protection Commissioner („Schrems”), punctul 76. Vezi și proiectul de decizie, considerentul 105 și articolul 3 alineatul (5).