2025/1382

18.7.2025

DECIZIA DE PUNERE ÎN APLICARE (UE) 2025/1382 A COMISIEI

din 15 iulie 2025

în temeiul Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului privind protecția adecvată a datelor cu caracter personal de către Organizația Europeană de Brevete

[notificată cu numărul C(2025) 4626]

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere 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 (Regulamentul general privind protecția datelor) ([1]), în special articolul 45 alineatul (3),

întrucât:

1. INTRODUCERE

(1) Regulamentul (UE) 2016/679 stabilește normele pentru transferul de date cu caracter personal de la operatori sau persoane împuternicite de operatori din Uniune către țări terțe și organizații internaționale, în măsura în care astfel de transferuri intră în domeniul său de aplicare. Normele privind transferurile internaționale de date sunt prevăzute în capitolul V (articolele 44-50) din regulamentul respectiv. Deși fluxul de date cu caracter personal către și dinspre țări și organizații internaționale situate în afara Uniunii este esențial pentru dezvoltarea comerțului transfrontalier și a cooperării internaționale, nivelul de protecție conferit datelor cu caracter personal în Uniune nu trebuie să fie diminuat de transferurile către țări terțe sau organizații internaționale ([2]).

(2) În temeiul articolului 45 alineatul (3) din Regulamentul (UE) 2016/679, Comisia poate decide, printr-un act de punere în aplicare, că o țară terță, un teritoriu sau unul sau mai multe sectoare specificate dintr-o țară terță sau o organizație internațională asigură un nivel de protecție adecvat. În astfel de condiții, transferurile de date cu caracter personal către o organizație internațională se pot realiza fără a fi necesar să se obțină autorizări suplimentare, astfel cum se prevede la articolul 45 alineatul (1) și în considerentul 103 din Regulamentul (UE) 2016/679.

(3) În conformitate cu articolul 45 alineatul (2) din Regulamentul (UE) 2016/679, adoptarea unei decizii privind caracterul adecvat al nivelului de protecție trebuie să se bazeze pe o analiză cuprinzătoare a regimului juridic al organizației internaționale, în ceea ce privește atât normele aplicabile importatorilor de date, cât și limitările și garanțiile referitoare la accesul autorităților publice la datele cu caracter personal. În evaluarea sa, Comisia trebuie să stabilească dacă organizația internațională în cauză garantează un nivel de protecție „în esență echivalent” cu cel asigurat în cadrul Uniunii ([3]). Standardul în raport cu care este evaluată „echivalența în esență” este cel stabilit de legislația Uniunii, în special de Regulamentul (UE) 2016/679, precum și de jurisprudența Curții de Justiție a Uniunii Europene ([4]). „Criteriile de referință privind caracterul adecvat al nivelului de protecție” ale Comitetului european pentru protecția datelor (CEPD) sunt, de asemenea, importante în acest sens pentru a oferi clarificări suplimentare cu privire la standardul respectiv, precum și orientări în această privință ([5]).

([1]) JO L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.
([2]) A se vedea considerentul 101 din Regulamentul (UE) 2016/679.
([3]) A se vedea considerentul 104 din Regulamentul (UE) 2016/679.
([4]) A se vedea cauza C-311/18, Facebook Ireland și Schrems („hotărârea Schrems II”), ECLI:EU:C:2020:559, punctul 94.
([5]) Comitetul european pentru protecția datelor, „Criterii de referință privind caracterul adecvat al nivelului de protecție”, WP 254 rev. 01., disponibile la adresa https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

(4) Astfel cum a clarificat Curtea de Justiție, nu se poate impune ca o țară terță sau o organizație individuală să asigure un nivel de protecție identic cu cel garantat în ordinea juridică a Uniunii ([6]). În special, mijloacele la care țara terță sau organizația internațională în cauză recurge pentru protecția datelor cu caracter personal pot fi diferite de cele puse în aplicare în Uniune, cu condiția ca acestea să se dovedească în practică efective în scopul de a asigura un nivel de protecție adecvat ([7]). Prin urmare, standardul caracterului adecvat nu necesită o reproducere punct cu punct a normelor Uniunii. Mai curând, testul constă în a se stabili dacă, prin fondul drepturilor la viață privată și al garanțiilor în materie de protecție a datelor (inclusiv în ceea ce privește punerea lor efectivă în aplicare, supravegherea și asigurarea respectării acestora), precum și prin circumstanțele referitoare la transferul datelor cu caracter personal, sistemul străin în cauză, în ansamblul său, oferă nivelul de protecție necesar ([8]).

(5) Comisia a analizat cadrul juridic și practica Organizației Europene de Brevete. Pe baza constatărilor prezentate în considerentele 7-100, Comisia concluzionează că Organizația Europeană de Brevete asigură un nivel de protecție adecvat pentru datele cu caracter personal care intră în domeniul de aplicare al Regulamentului (UE) 2016/679, transferate din Uniune către Organizația Europeană de Brevete.

(6) În temeiul prezentei decizii, transferurile de la operatorii și persoanele împuternicite de operatori din Uniune către Organizația Europeană de Brevete pot avea loc fără a fi necesară obținerea unei autorizări suplimentare. Prezenta decizie nu ar trebui să aducă atingere aplicării directe a Regulamentului (UE) 2016/679 pentru astfel de entități în cazul în care sunt îndeplinite condițiile privind domeniul de aplicare teritorial prevăzut la articolul 3 din regulamentul respectiv.

2. NORMELE APLICABILE PRELUCRĂRII DATELOR CU CARACTER PERSONAL

2.1. Organizarea și sarcinile Organizației Europene de Brevete

(7) Organizația Europeană de Brevete este o organizație interguvernamentală, înființată la 7 octombrie 1977 pe baza Convenției brevetului european (CBE). Organizația își are sediul la München și are 39 de state contractante, cuprinzând toate statele membre ale Uniunii, Islanda, Norvegia și Liechtenstein, precum și Albania, Macedonia de Nord, Monaco, San Marino, Serbia, Elveția, Muntenegru, Regatul Unit și Turcia ([9]).

(8) Organizația are personalitate juridică ([10]) și este formată din două organe ([11]): Oficiul European de Brevete (Oficiul) și Consiliul de administrație. Principala sarcină a Organizației Europene de Brevete este acordarea brevetelor europene ([12]) în conformitate cu CBE, care este efectuată de Oficiu sub supravegherea Consiliului de administrație. Consiliul de administrație este format din reprezentanți ai statelor contractante și exercită competențe legislative în numele Organizației Europene de Brevete. Acesta este, de asemenea, responsabil pentru aspectele legate de politici și supraveghează activitățile Oficiului ([13]). Oficiul, care acționează în calitate de organ executiv al Organizației Europene de Brevete, este condus de un președinte ([14]), care administrează Oficiul (președintele) și răspunde în fața Consiliului de administrație ([15]). Printre altele, președintele pregătește și execută bugetul Oficiului, numește și supraveghează personalul Oficiului, își exercită autoritatea disciplinară asupra personalului, asigură funcționarea Oficiului, inclusiv adoptarea de instrucțiuni administrative interne și informarea publicului, și poate prezenta Consiliului de administrație orice propunere

([6]) Cauza C-362/14, Schrems („hotărârea Schrems I”), ECLI:EU:C:2015:650, punctul 73.
([7]) Hotărârea Schrems I, punctul 74.
([8]) Hotărârea Schrems I, punctul 75.
([9]) Se reflectă numărul de state contractante la nivelul lunii februarie 2025.
([10]) Articolul 5 alineatul (1) din CBE.
([11]) Articolul 4 alineatul (2) din CBE.
([12]) În fiecare dintre statele contractante pentru care este acordat, un brevet european are, în principiu, efectul unui brevet național acordat de statul respectiv și este supus acelorași condiții precum acesta [a se vedea articolul 2 alineatul (2) din CBE].
([13]) Articolele 26 și 33 din CBE.
([14]) Președintele este numit de Consiliul de administrație și reprezintă Organizația Europeană de Brevete pe plan extern [articolul 5 alineatul (3) din CBE].
([15]) Articolul 10 alineatul (1) din CBE.

de modificare a convenției, a regulamentelor generale sau a deciziilor care intră în sfera sa de competență ([16]). Oficiul este format din diverse departamente, care includ o secție de primire, o divizie juridică, diviziile de examinare și de opoziție, precum și camerele de recurs (un organism intern independent în fața căruia pot fi atacate deciziile luate de Organizația Europeană de Brevete în contextul procedurii de acordare a brevetelor) ([17]).

(9) În îndeplinirea sarcinilor sale, Organizația Europeană de Brevete primește date cu caracter personal de la o serie de actori diferiți din Uniune. Cererile de brevet european ([18]) sunt depuse, în mod continuu, la Organizația Europeană de Brevete de către solicitanții de brevete sau sunt transmise acesteia de către oficiile naționale de brevete din statele membre ([19]). De asemenea, Organizația Europeană de Brevete primește și prelucrează date cu caracter personal în contextul sarcinilor care îi sunt încredințate în temeiul Regulamentului (UE) nr. 1257/2012 al Parlamentului European și al Consiliului ([20]). Printre aceste sarcini se numără primirea și examinarea cererilor de efect unitar al brevetelor europene, colectarea taxelor anuale și înregistrarea efectului unitar ([21]). În acest context, Organizația Europeană de Brevete primește, de asemenea, cereri cu privire la recursurile în curs înaintea camerelor de recurs ale Oficiului ([22]), adresate de Curtea unică în materie de brevete, care pot include date cu caracter personal necesare pentru identificarea cazului relevant ([23]).

(10) În mod similar, Organizația Europeană de Brevete primește date cu caracter personal conținute în cererile internaționale de brevete atunci când acționează în temeiul Tratatului de cooperare în domeniul brevetelor, un tratat internațional care permite solicitanților să obțină brevete cu efecte pentru toate statele contractante în temeiul Tratatului de cooperare în domeniul brevetelor ([24]). Organizația Europeană de Brevete acționează în calitate de autoritate internațională de cercetare în temeiul Tratatului de cooperare în domeniul brevetelor și, în această calitate, examinează posibilitatea de brevetare a invențiilor divulgate în cererile internaționale, ceea ce îi ajută pe solicitanți să stabilească dacă să depună sau nu o cerere de examinare pe fond la nivel național/la nivelul Uniunii ([25]).

(11) În plus, Organizația Europeană de Brevete cooperează îndeaproape cu oficiile naționale de brevete din toate statele membre în cadrul unei „rețele europene de brevete” și, în acest context, face schimb de date cu caracter personal cu acestea, de exemplu atunci când oferă cursuri de formare și servicii informatice pentru a sprijini și a consolida cooperarea în temeiul CBE. În mod similar, aceasta a încheiat cu statele membre acorduri bilaterale de cooperare care implică schimbul de date cu caracter personal, de exemplu în contextul instituirii de grupuri de lucru, al detașării și al delegării de experți tehnici etc. De asemenea, aceasta cooperează îndeaproape cu Oficiul Uniunii Europene pentru Proprietate Intelectuală (EUIPO), de exemplu prin organizarea de cursuri de formare comune și de evenimente de sensibilizare a opiniei publice, precum și prin detașarea de experți.

([16]) Articolul 10 alineatul (2) din CBE.

([17]) Membrii camerelor de recurs sunt numiți de Consiliul de administrație (la propunerea președintelui) și funcționează independent [articolul 11 alineatul (3) și articolul 23 din CBE].

([18]) Printre acestea se numără, de exemplu, numele, adresa, cetățenia și numărul de telefon al solicitanților, numele și adresa inventatorilor și ale reprezentanților în materie de brevete, numele și informațiile financiare ale persoanei care efectuează plățile etc. Organizația Europeană de Brevete poate obține date cu caracter personal suplimentare dacă o parte terță se opune acordării unui brevet, caz în care informații suplimentare, cum ar fi observații, dovezi și declarații scrise ale părților terțe, pot fi comunicate Organizației Europene de Brevete [a se vedea Regulamentul de punere în aplicare a CBE, de exemplu norma 41 alineatul (2), norma 143 alineatul (1) litera (h), norma 92 alineatul (2) litera (c), norma 19 alineatul (1), norma 53 alineatul (1) etc.]. A se vedea, de asemenea, articolul 9 din Decizia președintelui privind procedura de acordare a brevetelor.

([19]) O cerere de brevet european poate fi depusă la oficiul central pentru proprietate industrială sau la altă autoritate competentă a unui stat contractant. După verificarea cererii din perspectiva securității sau în temeiul altor cerințe naționale, autoritatea națională o transmite Organizației Europene de Brevete.

([20]) Regulamentul (UE) nr. 1257/2012 al Parlamentului European și al Consiliului din 17 decembrie 2012 de punere în aplicare a unei cooperări consolidate în domeniul creării unei protecții unitare prin brevet (JO L 361, 31.12.2012, p. 1, ELI: http://data.europa.eu/eli/reg/2012/1257/oj).

([21]) Brevetele unitare cu efect unitar pentru toate statele membre participante sunt înregistrate la nivel central la Organizația Europeană de Brevete, fără a fi necesare demersuri administrative suplimentare la nivel național (astfel cum este necesar pentru brevetele europene).

([22]) În decembrie 2024, Organizația Europeană de Brevete a adoptat o normă privind un mecanism independent de supraveghere a prelucrării datelor cu caracter personal de către camera de recurs în exercițiul funcției sale judiciare. Aceasta este disponibilă la adresa https://www.epo.org/en/about-us/transparency-portal?search_description=CA%2FD+19%2F24&op=&sort_by=most&items_per_page=10.

([23]) Curtea unică în materie de brevete a fost instituită pe baza Acordului privind Curtea unică în materie de brevete (JO C 175, 20.6.2013, p. 1) și are competență exclusivă, printre altele, în ceea ce privește brevetele europene (sub rezerva unei perioade tranzitorii) și brevetele europene cu efect unitar (de exemplu în ceea ce privește acțiunile în constatarea încălcării sau a riscului de încălcare și mijloacele de protecție conexe, acțiunile în constatarea inexistenței unei încălcări, acțiunile în vederea obținerii unor măsuri și ordine provizorii și asiguratorii, acțiunile în revocare și cererile reconvenționale în revocare). Curtea unică în materie de brevete are, de asemenea, competență exclusivă în ceea ce privește deciziile Organizației Europene de Brevete în îndeplinirea atribuțiilor sale privind protecția unitară prin brevet.

([24]) Pentru o prezentare generală a procedurii în temeiul Tratatului de cooperare în domeniul brevetelor, a se vedea *PCT Applicant's Guide – Introduction to the International Phase* (Ghidul solicitantului în temeiul Tratatului de cooperare în domeniul brevetelor – Introducere cu privire la etapa internațională), disponibil la adresa https://www.wipo.int/pct/en/guide/index.html, în special capitolul 3, precum și *Guide for applicants: PCT procedure before the EPO (Euro-PCT Guide)* (Ghid pentru solicitanți: procedura în temeiul Tratatului de cooperare în domeniul brevetelor desfășurată înaintea Organizației Europene de Brevete – Ghidul Euro-PCT), a șaisprezecea ediție, 1 ianuarie 2023, disponibil la adresa https://www.epo.org/en/legal/guide-europct/2023/index.html. Pentru categoriile de date cu caracter personal prelucrate de Organizația Europeană de Brevete în cadrul procedurilor în temeiul Tratatului de cooperare în domeniul brevetelor, a se vedea în special secțiunea 9 literele (a), (d), (h), (i), (j), (l), (m), (n) și (p) din anexa la Decizia președintelui Oficiului European de Brevete din 13 decembrie 2021 privind prelucrarea datelor cu caracter personal în procedurile de acordare a brevetelor și în procedurile conexe (JO, Oficiul European de Brevete 2021, A98).

([25]) De asemenea, în acest caz, este posibil ca o cerere de brevet să trebuiască să fie transferată Organizației Europene de Brevete de la oficiul central pentru proprietate industrială sau de la o altă autoritate competentă a unui stat contractant în temeiul Tratatului de cooperare în domeniul brevetelor.

(12) În sfârșit, Organizația Europeană de Brevete are contracte cu mai mulți furnizori de servicii din Uniune care acționează în calitate de persoană împuternicită de operator în sensul articolului 4 punctul 8 din Regulamentul (UE) 2016/679 și transferă date cu caracter personal către Organizația Europeană de Brevete.

2.2. **Cadrul juridic aplicabil și normele privind protecția datelor**

(13) Legislația primară care reglementează activitățile Organizației Europene de Brevete este stabilită printr-un tratat internațional, și anume Convenția brevetului european, și, în cazul în care Organizația Europeană de Brevete acționează în temeiul Tratatului de cooperare în domeniul brevetelor, prin acesta din urmă. La un al doilea nivel al ierarhiei normelor aplicabile Organizației Europene de Brevete sunt actele juridice adoptate de Consiliul de administrație sau, în ceea ce privește Tratatul de cooperare în domeniul brevetelor, de Adunarea în temeiul Tratatului de cooperare în domeniul brevetelor. Legislația secundară aplicabilă Organizației Europene de Brevete include Regulamentul de punere în aplicare a CBE și așa-numitul statut al personalului (care reglementează aspecte legate de personalul Organizației Europene de Brevete, inclusiv drepturile și obligațiile acestuia) ([26]). Dreptul la protecția datelor cu caracter personal este prevăzut la articolul 1B din Statutul personalului ([27]), care conține, de asemenea, unele dispoziții esențiale ale cadrului de protecție a datelor al Organizației Europene de Brevete, și anume în ceea ce privește domeniul de aplicare al cadrului de protecție a datelor, protecția categoriilor speciale de date și exercitarea drepturilor de către persoanele fizice. Articolul 2 alineatul (1) și articolul 32A din Statutul personalului instituie mecanisme independente de supraveghere (responsabilul cu protecția datelor și Comitetul pentru protecția datelor) pentru a supraveghea respectarea normelor privind protecția datelor ([28]).

(14) Aceleași cerințe de fond care reglementează protecția datelor cu caracter personal se aplică și Consiliului de administrație și Oficiului, precum și tuturor serviciilor acestora. În special, prelucrarea datelor cu caracter personal de către Oficiu este reglementată de normele de punere în aplicare a articolelor 1B și 32A din Statutul personalului pentru angajații permanenți și alți angajați ai Oficiului European de Brevete în ceea ce privește protecția datelor cu caracter personal (Normele privind protecția datelor – DPR), care au fost adoptate de Consiliul de administrație ([29]). Prelucrarea datelor cu caracter personal de către Consiliul de administrație face obiectul Normelor privind protecția datelor ale Consiliului de administrație, care aplică Normele privind protecția datelor *mutatis mutandis* ([30]). În situațiile în care prezenta decizie se referă la Normele privind protecția datelor, trimiterile respective includ cerințele corespunzătoare care se aplică în cazul Consiliului de administrație, secretariatului și comitetelor acestuia. Structura și conținutul Normelor privind protecția datelor sunt strâns aliniate la cadrul Uniunii privind protecția datelor ([31]). În special, acesta împărtășește multe puncte comune cu Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([32]), care stabilește cerințele de protecție a datelor pentru instituțiile și organele Uniunii și, prin urmare, este bine adaptat la structura și caracteristicile specifice ale organizațiilor internaționale, reflectând totodată îndeaproape Regulamentul (UE) 2016/679.

([26]) Articolul 33 din CBE.

([27]) A se vedea în special articolul 1B alineatul (1) din Statutul personalului, care prevede că „Oficiul depune eforturi pentru a asigura respectarea drepturilor fundamentale la viață privată și la protecția datelor cu caracter personal ale tuturor persoanelor fizice ale căror date sunt prelucrate de Oficiu și pentru a garanta răspunderea în această privință”. A se vedea de asemenea articolul 1 alineatul (1) din Normele privind protecția datelor, care explică faptul că Normele privind protecția datelor oferă cadrul juridic necesar pentru a se asigura că „drepturile fundamentale ale persoanelor fizice la viață privată și la protecția datelor lor cu caracter personal prelucrate de Oficiu sunt respectate”.

([28]) A se vedea, de asemenea, articolele 47 și 48 din Normele privind protecția datelor.

([29]) Normele privind protecția datelor (de la p. 495), disponibile la adresa https://report-archive.epo.org/files/babylon/service_regulations_en.pdf. Normele privind protecția datelor se aplică, de asemenea, camerelor de recurs ale Oficiului, cu excepția procedurii de recurs desfășurate înaintea Comitetului pentru protecția datelor, care nu se aplică prelucrării datelor cu caracter personal de către camere în exercițiul funcției lor judiciare [articolul 2 alineatul (6) din Normele privind protecția datelor]. Pentru aceste activități, Normele privind protecția datelor impun camerelor să instituie un mecanism independent separat de reexaminare.

([30]) Normele privind protecția datelor ale Consiliului de administrație, disponibile la adresa https://link.epo.org/ac-document/CA/D%202/23%20-%20En.pdf. Singurul aspect cu privire la care Normele privind protecția datelor ale Consiliului de administrație diferă de Normele privind protecția datelor se referă la adaptările care vizează structura specifică a Consiliului de administrație, și anume prin înlocuirea trimiterilor la președinte cu trimiteri la președintele Consiliului de administrație. În plus, s-au adoptat norme separate – Normele privind protecția datelor ale Comitetului restrâns – pentru așa-numitul Comitet restrâns al Consiliului de administrație. Acest comitet este compus din statele contractante ale Organizației Europene de Brevete și organizațiile de utilizatori și a fost instituit prin articolul 9 alineatul (2) din Regulamentul (UE) nr. 1257/2012 și prin articolul 145 din CBE pentru a supraveghea activitățile Oficiului în contextul procedurii de brevet unitar. Normele privind protecția datelor ale Comitetului restrâns aplică Normele privind protecția datelor ale Consiliului de administrație (care, la rândul lor, aplică Normele privind protecția datelor) în contextul prelucrării datelor cu caracter personal de către Comitetul restrâns (a se vedea https://link.epo.org/web/about-us/governance/SC_D_1_23_en.pdf). De asemenea, Normele privind protecția datelor ale Comitetului restrâns diferă de normele Consiliului de administrație și ale Oficiului numai în ceea ce privește trimiterea la președintele comitetului (în locul președintelui consiliului sau al președintelui).

([31]) Normele Organizației Europene de Brevete privind protecția datelor: https://www.epo.org/en/about-us/office/data-protection-and-privacy.

([32]) 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 (JO L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(15) În ceea ce privește prelucrarea datelor de către Oficiu, președintele a emis și alte instrumente obligatorii din punct de vedere juridic, cum ar fi circulare, decizii și instrucțiuni administrative interne ([33]). În special, Normele privind protecția datelor sunt completate de Decizia din 13 decembrie 2021 a președintelui privind prelucrarea datelor cu caracter personal în procedurile de acordare a brevetelor și în procedurile conexe (Decizia privind procedurile de acordare a brevetelor și procedurile conexe) ([34]), Decizia din 7 decembrie 2022 privind prelucrarea datelor cu caracter personal în cadrul procedurilor referitoare la brevetele europene cu efect unitar (Decizia privind brevetele unitare) ([35]), Decizia din 17 noiembrie 2022 privind țările și entitățile despre care se consideră că asigură o protecție adecvată a datelor cu caracter personal ([36]), Decizia din 2 mai 2024 de identificare a unităților operaționale ale Oficiului care acționează în calitate de operatori delegați ([37]) și Circulara nr. 420 de punere în aplicare a articolului 25 din Normele privind protecția datelor în ceea ce privește restricțiile referitoare la drepturile persoanelor vizate (Circulara nr. 420) ([38]). În special în ceea ce privește prelucrarea datelor în contextul procedurilor de acordare a brevetelor, este important de remarcat faptul că respectivele cerințe pentru prelucrarea datelor cu caracter personal prevăzute direct în CBE și în Tratatul de cooperare în domeniul brevetelor prevalează asupra Normelor privind protecția datelor. Interacțiunea dintre CBE și Tratatul de cooperare în domeniul brevetelor, pe de o parte, și Normele privind protecția datelor, pe de altă parte, este clarificată în Decizia privind procedurile de acordare a brevetelor și procedurile conexe ([39]) și în Decizia privind brevetele unitare. Cerințele specifice de protecție a datelor care decurg direct din CBE și Tratatul de cooperare în domeniul brevetelor sunt evaluate în considerentele 55-59. Normele privind protecția datelor și instrumentele sale complementare sunt obligatorii din punct de vedere juridic și executorii și pot fi invocate de persoane fizice înaintea unor mecanisme independente de recurs, astfel cum se descrie în considerentele 89-96.

(16) Normele prevăzute în instrumentele juridice menționate în considerentul 15 sunt operaționalizate suplimentar în instrumentele emise de responsabilul cu protecția datelor (a se vedea considerentele 83-88) ([40]), care se aplică Oficiului și Consiliului de administrație, precum și tuturor serviciilor acestora ([41]).

2.3. **Domeniul de aplicare material și personal al Normelor privind protecția datelor**

(17) În temeiul Normelor privind protecția datelor și al Statutului personalului ([42]), toți angajații Organizației Europene de Brevete trebuie să respecte Normele privind protecția datelor atunci când prelucrează date cu caracter personal. Domeniul de aplicare material și personal al Normelor privind protecția datelor este stabilit de termenii „date cu caracter personal", „prelucrare", „operator", „operator delegat" și „persoană împuternicită de operator" definiți în acesta.

2.3.1. ***Definiția datelor cu caracter personal și a prelucrării***

(18) Definițiile termenilor „date cu caracter personal" și „prelucrare" din Normele privind protecția datelor sunt identice cu cele din Regulamentul (UE) 2016/679 ([43]). Normele privind protecția datelor se aplică oricărei prelucrări de date cu caracter personal de către Organizația Europeană de Brevete, indiferent dacă o astfel de prelucrare se referă la datele cu caracter personal ale propriilor angajați sau la datele altor persoane fizice ([44]). Datele care au fost

([33]) Articolul 10 din CBE. A se vedea, de asemenea, articolul 1 alineatul (2) litera (a) din Normele privind protecția datelor.

([34]) https://www.epo.org/en/legal/official-journal/2021/12/a98.html. O decizie similară a fost adoptată în ceea ce privește prelucrarea datelor de către președintele camerelor de recurs în cadrul procedurii de recurs desfășurate înaintea camerelor de recurs, și anume Decizia din 14 iulie 2023 privind prelucrarea datelor cu caracter personal în cadrul procedurilor de recurs desfășurate înaintea camerelor de recurs, disponibilă la adresa https://www.epo.org/en/legal/official-journal/2023/07/a73.html.

([35]) Decizia din 7 decembrie 2022 privind prelucrarea datelor cu caracter personal în cadrul procedurilor referitoare la brevetele europene cu efect unitar, disponibilă la adresa https://www.epo.org/en/legal/official-journal/2022/12/a112.html.

([36]) https://epo.org/en/legal/official-journal/2022/12/a111.html. Astfel cum a fost modificată prin Decizia din 11 mai 2023 (JO, Oficiul European de Brevete 2023, A57), disponibilă la adresa https://www.epo.org/en/legal/official-journal/2023/06/a57.html.

([37]) https://link.epo.org/web/en-decision-of-the-president-on-delegated-controllers.pdf. Această decizie se actualizează cel puțin o dată pe an.

([38]) Circulara nr. 420 de punere în aplicare a articolului 25 din Normele privind protecția datelor, disponibilă la adresa https://link.epo.org/web/circular_420_en.pdf.

([39]) În ceea ce privește prelucrarea datelor cu caracter personal de către camerele de recurs în cadrul procedurilor de recurs, această interacțiune este clarificată în Decizia președintelui camerelor de recurs privind prelucrarea datelor cu caracter personal în cadrul procedurilor de recurs desfășurate înaintea camerelor de recurs.

([40]) A se vedea, de exemplu, trimiterea la documentele operaționale emise de responsabilul cu protecția datelor de la articolul 1 alineatul (2) litera (c) din Normele privind protecția datelor, care au fost aprobate de președinte și, prin urmare, au devenit obligatorii.

([41]) A se vedea articolul 1 alineatul (6) și articolul 12 alineatul (5) din Normele privind protecția datelor ale Consiliului de administrație.

([42]) Articolul 2 alineatul (2) din Normele privind protecția datelor și articolul 1 din Statutul personalului.

([43]) Articolul 3 alineatul (1) literele (a) și (b) din Normele privind protecția datelor și articolul 4 alineatele (1) și (2) din RGPD.

([44]) Articolul 1B alineatul (2) din Statutul personalului și articolul 2 alineatele (2) și (3) din Normele privind protecția datelor. A se vedea, de asemenea, definiția „persoanei vizate" [articolul 3 alineatul (1) litera (w) din Normele privind protecția datelor], și anume „orice persoană fizică identificată sau identificabilă, indiferent dacă persoana respectivă este sau nu un angajat al Oficiului". Pentru a se determina dacă o persoană fizică este identificabilă, trebuie să se ia în considerare toate mijloacele, cum ar fi individualizarea, pe care este probabil, în mod rezonabil, să le utilizeze fie operatorul, fie o altă persoană, în scopul identificării, în mod direct sau indirect, a persoanei fizice respective.

pseudonimizate ([45]) sunt, de asemenea, considerate date cu caracter personal, în timp ce datele persoanelor decedate sau ale persoanelor juridice sau informațiile anonime ([46]) nu sunt tratate ca date cu caracter personal în temeiul Normelor privind protecția datelor ([47]).

(19) Normele privind protecția datelor se aplică prelucrării datelor cu caracter personal de către Organizația Europeană de Brevete, efectuate total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență sau care sunt destinate să facă parte dintr-un sistem de evidență ([48]).

2.3.2. ***Operatorul, operatorul delegat și persoana împuternicită de operator***

(20) Normele privind protecția datelor definesc un „operator" ca fiind „o entitate, și anume Oficiul European de Brevete, care, singură sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal" ([49]). În principiu, președintele acționează în calitate de operator pentru operațiunile de prelucrare a datelor efectuate de Oficiu ([50]). Același lucru este valabil și pentru Consiliul de administrație (în acest caz, președintele acționând în calitate de operator), pentru camerele de recurs în exercițiul funcției lor judiciare [în acest caz, președintele acestora acționând în calitate de operator ([51])] și Comitetul restrâns [în acest caz, președintele acționând în calitate de operator ([52])]. Operatorul poate delega această competență unităților operaționale, reprezentate de un director de nivel superior ([53]). În astfel de cazuri, unitățile operaționale acționează în calitate de „operatori delegați" ([54]), definind scopul (de exemplu motivul, justificarea și nevoile operaționale), precum și mijloacele unei operațiuni de prelucrare și asigurându-se că toate operațiunile de prelucrare care implică date cu caracter personal respectă dispozițiile Normelor privind protecția datelor ([55]). În astfel de cazuri, operatorul rămâne responsabil de prelucrarea datelor cu caracter personal. Normele privind protecția datelor prevăd, de asemenea, un scenariu de „exercitare în comun a competenței de operator", în cadrul căruia un operator stabilește scopul și mijloacele de prelucrare împreună cu unul sau mai mulți operatori din afara Organizației Europene de Brevete ([56]).

([45]) Cu alte cuvinte, prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile – a se vedea articolul 3 alineatul (1) litera (e) din Normele privind protecția datelor.

([46]) Cu alte cuvinte, „informații care nu se referă la o persoană fizică identificată sau identificabilă sau la date cu caracter personal făcute anonime în așa fel încât persoana vizată să nu fie sau să nu mai fie identificabilă" – a se vedea articolul 3 alineatul (1) litera (r) din Normele privind protecția datelor. În temeiul articolului 13 alineatul (1) din Normele privind protecția datelor, operatorul nu este obligat să păstreze, să obțină sau să prelucreze informații suplimentare pentru a identifica o persoană fizică în scopul unic al respectării Normelor privind protecția datelor, în cazul în care scopurile în care sunt prelucrate datele nu necesită sau nu mai necesită identificarea unei persoane fizice.

([47]) Articolul 2 alineatul (4) din Normele privind protecția datelor. În ceea ce privește prelucrarea datelor cu caracter personal în scopuri de arhivare (în exercitarea legitimă a autorității publice a Organizației Europene de Brevete), în scopuri de cercetare științifică sau istorică ori în scopuri statistice, Normele privind protecția datelor impun instituirea unor măsuri tehnice și organizatorice, printre altele, pentru a asigura respectarea principiului reducerii la minimum a datelor și, în cazul în care scopul prelucrării poate fi atins în acest mod, pentru a prelucra datele într-un mod care să nu mai permită identificarea persoanei fizice în cauză (articolul 14 din Normele privind protecția datelor).

([48]) Articolul 1B alineatul (3) din Statutul personalului și articolul 2 alineatul (1) din Normele privind protecția datelor. Termenul „sistem de evidență a datelor" este definit ca „orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice" – a se vedea articolul 3 alineatul (1) din Normele privind protecția datelor.

([49]) Articolul 3 alineatul (1) litera (g) din Normele privind protecția datelor. Atunci când se utilizează termenul „operator" în prezenta decizie, acesta se referă fie la Organizația Europeană de Brevete, fie la operatorii delegați.

([50]) Articolul 10 alineatul (2) din CBE și articolul 28 alineatul (1) din Normele privind protecția datelor.

([51]) Articolul 28 alineatul (2) din Normele privind protecția datelor. Acest lucru rezultă în mod specific dintr-o delegare de competențe din partea președintelui Oficiului – a se vedea https://www.epo.org/en/legal/official-journal/2021/etc/se1/p175.html. Pentru alte activități (în cazul în care camerele nu acționează în exercițiul funcției lor judiciare), președintele camerelor acționează în calitate de operator delegat pentru președintele Oficiului.

([52]) A se vedea articolul 1 alineatul (4) punctul 5 din Normele privind protecția datelor ale Consiliului de administrație și articolul 13a alineatul (2) din Regulamentul de procedură al Comitetului restrâns.

([53]) Articolul 28 alineatul (3) din Normele privind protecția datelor.

([54]) A se vedea articolul 3 alineatul (1) litera (h) din Normele privind protecția datelor. Persoana care reprezintă unitatea operațională trebuie să fie un director de nivel superior, în mod normal cel puțin un director principal. Lista operatorilor delegați este făcută publică (a se vedea, de exemplu, https://link.epo.org/web/en-decision-of-the-president-on-delegated-controllers.pdf și https://link.epo.org/web/decision_of_the_president_of_the_boards_of_appeal_appointing_a_delegated_controller_en.pdf) și este actualizată periodic.

([55]) Atunci când prezenta decizie se referă la un „operator", această trimitere include operatorii delegați relevanți.

([56]) În acest caz, articolul 29 din Normele privind protecția datelor prevede obligația operatorului (delegat) de a stabili, în mod transparent, responsabilitățile respective ale ambelor părți în ceea ce privește respectarea obligațiilor care le revin în materie de protecție a datelor, în special în ceea ce privește exercitarea drepturilor persoanelor fizice și obligațiile în materie de transparență.

(21) Termenul „persoană împuternicită de operator” este definit identic în Normele privind protecția datelor și la articolul 4 punctul 8 din Regulamentul (UE) 2016/679, acesta fiind persoana fizică sau juridică, autoritatea publică, agenția sau orice altă entitate care prelucrează date cu caracter personal în numele operatorului ([57]). Operatorul este autorizat să apeleze doar la persoane împuternicite de operator care oferă garanții suficiente că vor fi puse în aplicare măsuri tehnice și organizatorice adecvate pentru a se asigura că prelucrarea îndeplinește cerințele din Normele privind protecția datelor ([58]). Relația dintre operator și o persoană împuternicită de operator trebuie să fie reglementată de un contract sau de un act juridic care să fie obligatoriu pentru persoana împuternicită de operator și care, printre altele, să stabilească obiectul, durata, natura și scopul prelucrării ([59]). Persoana împuternicită de operator este autorizată să prelucreze datele numai pe baza unor instrucțiuni documentate din partea operatorului. Persoana împuternicită de operator are obligația de a oferi asistență operatorului în îndeplinirea obligațiilor care îi revin în temeiul Normelor privind protecția datelor. Se interzice persoanei împuternicite de operator să angajeze subcontractanți fără autorizarea prealabilă a operatorului ([60]). Un acord standard de prelucrare a datelor este disponibil pentru operatorii delegați ([61]). În plus, în cazul în care o persoană împuternicită de operator este situată într-o țară terță, orice schimb de date cu caracter personal cu respectiva persoană împuternicită de operator trebuie, de asemenea, să respecte cerințele prevăzute de Normele privind protecția datelor pentru transferurile internaționale, astfel cum sunt descrise în considerentele 68-73 din prezenta decizie ([62]).

2.4. **Garanții, drepturi și obligații**

2.4.1. ***Legalitatea și echitatea prelucrării***

(22) Datele cu caracter personal ar trebui prelucrate în mod legal și echitabil.

(23) Aceste principii generale sunt prevăzute la articolul 4 alineatul (2) litera (a) din Normele privind protecția datelor într-un mod care poate fi considerat identic cu articolul 5 alineatul (1) litera (a) din Regulamentul (UE) 2016/679.

(24) Principiul legalității este dezvoltat suplimentar la articolul 5 din Normele privind protecția datelor, care enumeră temeiurile juridice pe baza cărora pot fi prelucrate datele cu caracter personal. Aceste temeiuri juridice sunt (a) necesitatea de a îndeplini o atribuție în exercitarea activităților oficiale ale Organizației Europene de Brevete ([63]) sau în exercitarea legitimă a autorității publice cu care este învestit operatorul, care include prelucrarea necesară pentru administrarea și funcționarea Oficiului ([64]), (b) necesitatea de a respecta o obligație legală care îi revine operatorului (de exemplu publicarea în Registrul european de brevete a informațiilor menționate într-o cerere de brevet) ([65]), (c) necesitatea de a executa un contract la care persoana vizată este parte sau de a face demersuri la cererea persoanei vizate înainte de încheierea unui contract, (d) consimțământul persoanei vizate sau (e) necesitatea de a proteja interesele vitale ale persoanei vizate sau ale unei alte persoane fizice.

([57]) Articolul 3 alineatul (1) litera (j) din Normele privind protecția datelor.

([58]) Articolul 30 alineatul (1) din Normele privind protecția datelor.

([59]) Articolul 30 alineatul (3) din Normele privind protecția datelor.

([60]) Articolul 30 alineatele (2)-(3) din Normele privind protecția datelor. O persoană împuternicită de operator care angajează un subcontractant are (contractual) obligația de a impune subcontractantului aceleași obligații în materie de protecție a datelor precum cele prevăzute în contractul dintre operator și persoana împuternicită de operator [articolul 30 alineatul (4) din Normele privind protecția datelor].

([61]) Anexa E la condițiile contractuale generale pentru Organizația Europeană de Brevete, https://link.epo.org/web/general_conditions_of_contract_en.pdf.

([62]) A se vedea articolul 8 alineatele (1), (2) și (5), coroborate cu articolul 9 alineatul (1) din Normele privind protecția datelor.

([63]) Aceasta se referă la atribuțiile îndeplinite în temeiul CBE și al Tratatului de cooperare în domeniul brevetelor sau la normele adoptate pe această bază (de exemplu Statutul personalului), care sunt necesare pentru îndeplinirea atribuțiilor Organizației Europene de Brevete în cadrul procedurii de acordare a brevetelor. A se vedea, de asemenea, punctul 5 subpunctul 1 din anexa la Decizia privind procedurile de acordare a brevetelor și procedurile conexe și dispozițiile relevante ale CBE, cum ar fi părțile IV și V. Pentru îndeplinirea atribuțiilor Organizației Europene de Brevete în contextul procedurii de acordare a brevetelor, Organizația Europeană de Brevete prelucrează date cu caracter personal pentru prelucrarea cererilor și a brevetelor, desfășurarea procedurilor de opoziție, comunicarea cu părțile la procedură (și, după caz, cu terții), menținerea Registrului european de brevete, elaborarea de rapoarte și statistici și schimbul de date cu statele contractante și cu Organizația Mondială a Proprietății Intelectuale (punctul 6 din anexa la Decizia privind procedurile de acordare a brevetelor și procedurile conexe).

([64]) Aceasta include atribuțiile președintelui Oficiului de a asigura funcționarea și administrarea eficace a Oficiului. A se vedea, de exemplu, articolul 10 din CBE, care descrie atribuțiile președintelui în ceea ce privește personalul, clădirile (și accesul la acestea) și gestionarea echipamentelor. Această abordare este în conformitate cu articolul 5 alineatul (1) litera (a) și cu considerentul 22 din Regulamentul (UE) 2018/1725. În mod similar, aceasta se referă la atribuțiile Consiliului de administrație în temeiul CBE, de exemplu de a stabili norme privind pensiile și reglementări financiare; a se vedea articolul 33 din CBE, norma 9 alineatul (2), norma 12 litera (c) și norma 122 alineatul (4) din Regulamentul de punere în aplicare a CBE. În ceea ce privește Comitetul restrâns, aceasta se referă la atribuțiile de supraveghere prevăzute la articolul 145 din CBE. În sfârșit, pentru camerele de recurs, aceasta se referă, de exemplu, la responsabilitatea examinării recursurilor formulate împotriva deciziilor altor părți ale Oficiului – a se vedea articolul 21 alineatul (1) din CBE.

([65]) A se vedea, de exemplu, norma 20 din Regulamentul de punere în aplicare a CBE.

(25) Consimțământul este definit în Normele privind protecția datelor în același mod precum în Regulamentul (UE) 2016/679, și anume ca fiind „orice 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 care o privesc să fie prelucrate” ([66]). Operatorului îi revine sarcina de a demonstra că persoana vizată și-a dat consimțământul ([67]). Atunci când se evaluează dacă respectivul consimțământ este dat în mod liber, ar trebui să se țină seama de aspectul dacă executarea unui contract este condiționată de consimțământul cu privire la prelucrarea unor date care nu sunt necesare pentru executarea acestui contract ([68]). Consimțământul nu poate fi considerat ca fiind dat în mod liber dacă persoana vizată nu dispune cu adevărat de libertatea de alegere sau nu este în măsură să refuze sau să își retragă consimțământul fără a fi prejudiciată ([69]). În plus, pentru ca acordarea consimțământului să fie în cunoștință de cauză, Normele privind protecția datelor prevăd ca persoana vizată să fie la curent cel puțin cu identitatea operatorului și cu scopurile prelucrării pentru care sunt destinate datele cu caracter personal ([70]). În sfârșit, o persoană vizată are dreptul de a-și retrage consimțământul în orice moment ([71]).

2.4.2. *Prelucrarea unor categorii speciale de date*

(26) În cazul în care sunt prelucrate „categorii speciale” de date, ar trebui să existe garanții specifice.

(27) Normele privind protecția datelor conțin dispoziții specifice în ceea ce privește prelucrarea categoriilor speciale de date cu caracter personal ([72]), care sunt definite în același mod precum în Regulamentul (UE) 2016/679, și anume ca fiind „date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate, date genetice ([73]) sau date biometrice ([74]) pentru identificarea unică a unei persoane fizice și date privind sănătatea ([75]) sau date privind viața sexuală sau orientarea sexuală ale unei persoane fizice” ([76]). În temeiul Normelor privind protecția datelor, prelucrarea categoriilor speciale de date este, în principiu, interzisă, cu excepția cazului în care se aplică o excepție specifică ([77]).

(28) Excepțiile specifice enumerate la articolul 11 alineatul (2) din Normele privind protecția datelor sunt similare celor de la articolul 9 alineatele (2) și (3) din Regulamentul (UE) 2016/679, cu câteva adaptări la cadrul juridic în care funcționează Organizația Europeană de Brevete. Prelucrarea categoriilor speciale de date cu caracter personal este permisă numai în circumstanțe specifice și limitate ([78]), și anume în cazul în care (1) persoana vizată și-a dat

([66]) Articolul 3 alineatul (1) litera (m) din Normele privind protecția datelor. A se vedea, de asemenea, articolul 7 alineatul (2) din Normele privind protecția datelor.
([67]) Articolul 7 alineatul (1) din Normele privind protecția datelor.
([68]) Articolul 7 alineatele (1), (5), (6) și (7) din Normele privind protecția datelor.
([69]) Articolul 7 alineatul (4) din Normele privind protecția datelor.
([70]) Articolul 7 alineatul (4) din Normele privind protecția datelor.
([71]) Articolul 7 alineatul (5) din Normele privind protecția datelor.
([72]) A se vedea, de exemplu, articolul 11 din Normele privind protecția datelor.
([73]) Definite ca „date cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea persoanei respective și care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana fizică în cauză” – a se vedea articolul 3 alineatul (1) litera (o) din Normele privind protecția datelor.
([74]) Definite ca „date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane fizice, cum ar fi imaginile faciale sau datele dactiloscopice” – a se vedea articolul 3 alineatul (1) litera (p) din Normele privind protecția datelor.
([75]) Cu alte cuvinte, date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia – a se vedea articolul 3 alineatul (1) litera (q) din Normele privind protecția datelor.
([76]) Articolul 11 alineatul (1) din Normele privind protecția datelor.
([77]) Articolul 11 alineatele (1) și (2) din Normele privind protecția datelor.
([78]) Normele privind protecția datelor permit, de asemenea, prelucrarea unor categorii speciale de date în scenarii specifice care se referă în principal la personalul Organizației Europene de Brevete și, prin urmare, sunt mai puțin relevante pentru datele transferate în baza prezentei decizii. În special, categoriile speciale de date pot fi prelucrate în cazul în care prelucrarea este autorizată printr-o dispoziție obligatorie din punct de vedere juridic aplicabilă Organizației Europene de Brevete [de exemplu CBE și instrumentele adoptate de Consiliul de administrație și de președinte – a se vedea articolul 3 alineatul (1) litera (y) din Normele privind protecția datelor] care prevede garanții adecvate pentru drepturile fundamentale și interesele persoanei vizate [articolul 11 alineatul (2) litera (b) din Normele privind protecția datelor] și este necesară în scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă și al securității sociale. În mod similar, prelucrarea poate avea loc atunci când este necesară din motive de interes public în domeniul sănătății publice [cum ar fi protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale, în temeiul dreptului național, care prevede măsuri adecvate și specifice pentru protejarea drepturilor și libertăților persoanei vizate, în special a secretului profesional – a se vedea articolul 11 alineatul (2) litera (g) din Normele privind protecția datelor]. În sfârșit, prelucrarea poate fi necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de tratament sau de asistență medicală sau socială, de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială sau de controalele și avizele medicale, în cazul în care aceste date sunt prelucrate de un cadru medical supus obligației de păstrare a secretului profesional sau de o altă persoană supusă unei obligații echivalente de păstrare a secretului [articolul 11 alineatul (3) din Normele privind protecția datelor].

consimțământul explicit în acest sens, (2) prelucrarea este necesară pentru protejarea intereselor vitale ale unei persoane fizice (atunci când persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul), (3) în cazul în care datele cu caracter personal sunt făcute publice în mod manifest de către persoana vizată, (4) prelucrarea este necesară pentru un scop specific legat de exercitarea activităților oficiale ale Organizației Europene de Brevete sau în exercitarea autorității legitime cu care este învestit operatorul ([79]) sau (5) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță.

(29) Pe lângă categoriile speciale de date cu caracter personal menționate în considerentul 27, Normele privind protecția datelor impun, de asemenea, măsuri de protecție specifice pentru prelucrarea datelor cu caracter personal referitoare la condamnări penale și infracțiuni, și anume permițând o astfel de prelucrare numai după consultarea prealabilă a Comitetului pentru protecția datelor sau în cazul în care prelucrarea este impusă de un instrument obligatoriu din punct de vedere juridic care prevede garanții adecvate pentru drepturile și libertățile persoanelor fizice ([80]).

2.4.3. ***Limitarea scopului***

(30) Datele cu caracter personal ar trebui să fie prelucrate într-un scop anume și să fie utilizate ulterior numai în măsura în care acest lucru nu este incompatibil cu scopul prelucrării.

(31) Acest principiu este garantat la articolul 4 alineatul (2) litera (b) din Normele privind protecția datelor, potrivit căruia datele cu caracter personal trebuie „să fie colectate în scopuri determinate, explicite și legitime și să nu fie prelucrate ulterior într-un mod incompatibil cu aceste scopuri”.

(32) Similar Regulamentului (UE) 2016/679, Normele privind protecția datelor permit prelucrarea ulterioară (indiferent de compatibilitatea scopului prelucrării ulterioare cu cel inițial) pe baza consimțământului explicit al persoanei vizate sau în temeiul dispozițiilor legale aplicabile ale Organizației Europene de Brevete ([81]). În acest din urmă caz, Normele privind protecția datelor impun ca prelucrarea să fie o măsură necesară și proporțională pentru a proteja un obiectiv de interes public general ([82]).

(33) În cazul în care prelucrarea ulterioară nu se bazează pe aceste două motive, Normele privind protecția datelor prevăd factorii care trebuie luați în considerare atunci când se evaluează compatibilitatea scopului prelucrării ulterioare cu scopul în care au fost colectate inițial datele cu caracter personal ([83]). Această abordare și factorii enumerați în Normele privind protecția datelor sunt identici cu cei prevăzuți la articolul 6 alineatul (4) din Regulamentul (UE) 2016/679 și la articolul 6 din Regulamentul (UE) 2018/1725 ([84]).

2.4.4. ***Exactitatea și reducerea la minimum a datelor***

(34) Datele cu caracter personal ar trebui să fie exacte și, dacă este necesar, actualizate. De asemenea, acestea ar trebui să fie adecvate, relevante și neexcesive în raport cu scopurile în care sunt prelucrate și, în principiu, păstrate pe o perioadă care nu depășește perioada necesară atingerii scopurilor în care sunt prelucrate datele cu caracter personal.

(35) Aceste principii sunt prevăzute la articolul 4 alineatul (2) literele (c), (d) și (e) din Normele privind protecția datelor în același mod ca în Regulamentul (UE) 2016/679.

([79]) De exemplu, în contextul recursurilor formulate împotriva brevetelor acordate, datele sensibile ar putea fi incluse în declarațiile martorilor sau în probele prezentate. Prelucrarea în temeiul acestei dispoziții poate avea loc, de asemenea, în cazul în care acest lucru este necesar în mod substanțial pentru administrarea și funcționarea Oficiului și pentru obligațiile care decurg din obligația Organizației Europene de Brevete de a coopera cu statele contractante (de exemplu necesitatea de a prelucra informațiile privind sănătatea ale personalului sau ale vizitatorilor în conformitate cu cerințele impuse de autoritățile de sănătate publică din statul unde își are sediul Organizația Europeană de Brevete). În orice caz, instrumentul juridic pe care se bazează prelucrarea trebuie să fie proporțional cu scopul urmărit, să respecte esența dreptului la protecția datelor și să prevadă măsuri adecvate și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate [articolul 11 alineatul (2) litera (f) din Normele privind protecția datelor].

([80]) Articolul 12 din Normele privind protecția datelor. Un scenariu posibil în care astfel de date ar fi prelucrate include proceduri disciplinare privind avocații specializați în brevete în fața comisiei de disciplină a Organizației Europene de Brevete (a se vedea, de exemplu, punctul A.7 din anexa la Decizia privind procedurile de acordare a brevetelor și procedurile conexe).

([81]) Articolul 6 alineatul (2) din Normele privind protecția datelor.

([82]) De exemplu, securitatea organizației, prevenirea, investigarea, depistarea și urmărirea penală a infracțiunilor, drepturile și libertățile altora etc. [a se vedea articolul 25 alineatul (1) din Normele privind protecția datelor].

([83]) Articolul 6 alineatul (3) din Normele privind protecția datelor.

([84]) În special, orice legătură între scopul colectării și scopul prelucrării ulterioare preconizate, contextul în care au fost colectate datele, tipul datelor și posibilele consecințe ale prelucrării ulterioare pentru persoanele fizice – a se vedea articolul 6 alineatul (3) din Normele privind protecția datelor.

(36) Datele cu caracter personal ar trebui prelucrate într-un mod care să le asigure securitatea, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale. În acest scop, operatorii economici ar trebui să ia măsurile tehnice sau organizatorice adecvate pentru a proteja datele cu caracter personal împotriva eventualelor amenințări. Aceste măsuri ar trebui să fie evaluate luând în considerare cunoștințele actuale și costurile aferente.

(37) Securitatea datelor este consacrată în cadrul juridic al Organizației Europene de Brevete prin principiul integrității și confidențialității prevăzut la articolul 4 alineatul (2) litera (f) și la articolul 33 din Normele privind protecția datelor, într-un mod aproape identic cu cel din Regulamentul (UE) 2016/679. În special, Normele privind protecția datelor impun asigurarea unui nivel de securitate corespunzător riscului prin măsuri tehnice și organizatorice adecvate, având în vedere stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și diferitele grade de probabilitate și gravitate a oricăror riscuri pentru drepturile și libertățile persoanelor fizice.

(38) În plus, Normele privind protecția datelor conțin cerințe specifice privind gestionarea și notificarea unei încălcări a securității datelor ([85]). În primul rând, operatorul are obligația de a notifica responsabilul cu protecția datelor cu privire la o încălcare a securității datelor fără întârzieri nejustificate (și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta), cu excepția cazului în care este puțin probabil ca încălcarea să genereze un risc pentru drepturile și libertățile persoanelor fizice ([86]). În mod similar, o persoană împuternicită de operator are obligația de a notifica operatorul cu privire la o încălcare fără întârzieri nejustificate ([87]). Notificarea trebuie să descrie, în special, natura încălcării, consecințele probabile ale acesteia și măsurile luate sau propuse pentru a remedia încălcarea ([88]). În cazul în care este probabil ca o încălcare a securității datelor să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul trebuie să informeze, de asemenea, persoana vizată fără întârziere cu privire la această încălcare ([89]). Informarea persoanei vizate trebuie să descrie natura încălcării securității datelor cu caracter personal într-un limbaj clar și simplu ([90]) și nu este necesară în cazul în care operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile și libertățile persoanelor vizate nu se mai materializează ([91]).

2.4.5. ***Transparență***

(39) Persoanele vizate ar trebui să fie informate cu privire la principalele caracteristici ale prelucrării datelor cu caracter personal ale acestora.

(40) În conformitate cu Normele privind protecția datelor, operatorul este obligat, în momentul obținerii datelor cu caracter personal, să furnizeze persoanelor fizice informații, în special în ceea ce privește identitatea și datele sale de contact (precum și datele de contact ale responsabilului cu protecția datelor), scopul prelucrării și temeiul juridic al acesteia, destinatarii sau categoriile de destinatari, faptul că intenționează să transfere datele în afara Organizației Europene de Brevete, precum și drepturile aplicabile și posibilitatea de a obține reparații ([92]). Același lucru este valabil și în cazul în care datele cu caracter personal sunt prelucrate în alt scop decât cel pentru care au fost colectate ([93]). Ambele obligații se aplică numai în măsura în care persoana fizică în cauză nu deține încă informațiile respective ([94]).

(41) Aceleași informații trebuie furnizate persoanelor vizate atunci când datele cu caracter personal nu sunt colectate direct de la acestea, împreună cu informații suplimentare privind sursa datelor cu caracter personal și categoriile de date în cauză ([95]). Aceste informații trebuie furnizate într-un termen rezonabil după obținerea datelor (dar nu mai mare de o lună), ținându-se seama de circumstanțele specifice în care sunt prelucrate datele ([96]). În cazul în care datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana vizată, aceleași informații ar trebui furnizate cel târziu în momentul primei comunicări cu persoana fizică respectivă ([97]). Informațiile menționate în considerentul 40 trebuie, de asemenea, să fie furnizate înainte de orice prelucrare ulterioară sau, în cazul în care se

([85]) „Încălcarea securității datelor" este definită ca „o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod sau la accesul neautorizat la acestea" – a se vedea articolul 3 alineatul (1) litera (n) din Normele privind protecția datelor.
([86]) Articolul 34 alineatul (1) din Normele privind protecția datelor.
([87]) Articolul 34 alineatul (2) din Normele privind protecția datelor.
([88]) Articolul 34 alineatele (1) și (3) din Normele privind protecția datelor.
([89]) Articolul 34 alineatul (6) din Normele privind protecția datelor.
([90]) Articolul 34 alineatul (6) din Normele privind protecția datelor.
([91]) Articolul 34 alineatul (8) din Normele privind protecția datelor.
([92]) Articolul 16 alineatele (1)-(2) din Normele privind protecția datelor.
([93]) Articolul 16 alineatul (3) din Normele privind protecția datelor.
([94]) Articolul 16 alineatul (4) din Normele privind protecția datelor.
([95]) Articolul 17 alineatele (1) și (2) din Normele privind protecția datelor.
([96]) Articolul 17 alineatul (3) litera (a) din Normele privind protecția datelor.
([97]) Articolul 17 alineatul (3) litera (b) din Normele privind protecția datelor.

intenționează divulgarea datelor către un alt destinatar, cel mai târziu la data la care datele cu caracter personal sunt divulgate unei părți terțe ([98]). Această obligație nu se aplică într-o serie de cazuri, și anume atunci când o persoană vizată deține deja informațiile în cauză, în cazul în care informațiile respective trebuie să rămână confidențiale ca urmare a unei obligații de păstrare a secretului profesional reglementată pe baza CBE și/sau a altor dispoziții legale aplicabile Organizației Europene de Brevete ([99]), în cazul în care furnizarea informațiilor respective se dovedește imposibilă sau ar implica eforturi disproporționate, în special în cazul prelucrării în scopul arhivării, al cercetării științifice sau istorice sau al statisticilor, în măsura în care aceasta ar face imposibilă sau ar afecta în mod grav realizarea obiectivelor prelucrării sau în cazul în care obținerea sau divulgarea informațiilor respective este prevăzută în mod expres în CBE sau în alte dispoziții legale aplicabile care prevăd măsuri adecvate pentru protejarea intereselor legitime ale persoanei vizate ([100]).

2.4.6. ***Drepturi individuale***

(42) Persoanele vizate ar trebui să aibă anumite drepturi care pot fi impuse operatorului sau persoanei împuternicite de operator, în special dreptul de acces la date, dreptul de rectificare, dreptul de a se opune prelucrării și dreptul la ștergerea datelor. În același timp, aceste drepturi pot face obiectul unor restricții, în măsura în care acestea sunt necesare și proporționale pentru a proteja obiectivele importante de interes public general.

2.4.6.1. *Drepturile prevăzute de Normele privind protecția datelor*

(43) Necesitatea de a facilita exercitarea drepturilor individuale este prevăzută la articolul 1B alineatul (4) din Statutul personalului. Pentru a continua punerea în aplicare a acestei cerințe, Normele privind protecția datelor oferă persoanelor fizice aceleași drepturi precum cele prevăzute în Regulamentul (UE) 2016/679, și anume dreptul de acces (articolul 18 din Normele privind protecția datelor), dreptul la rectificare (articolul 19 din Normele privind protecția datelor), dreptul la ștergerea datelor (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 unui proces decizional automatizat (articolul 24 din Normele privind protecția datelor).

(44) Normele privind protecția datelor stabilesc, de asemenea, dispoziții generale pentru gestionarea cererilor de exercitare a drepturilor din partea persoanelor fizice, impunând operatorului să comunice cu persoanele vizate utilizând un limbaj clar și simplu, într-o formă concisă, transparentă, inteligibilă și ușor accesibilă (în scris sau prin alte mijloace) ([101]). Operatorul trebuie să furnizeze persoanelor fizice informații cu privire la măsurile luate ca răspuns la o cerere, fără întârzieri nejustificate și, în orice caz, în termen de o lună de la primirea cererii (termen care poate fi prelungit cu încă două luni, dacă este necesar, având în vedere complexitatea cererilor și numărul acestora) ([102]). În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, operatorul poate refuza să dea curs cererii ([103]). În cazul în care operatorul nu dă curs unei cereri, acesta trebuie să informeze persoana fizică în cauză și să furnizeze informații cu privire la posibilitatea de a obține reparații ([104]).

([98]) Articolul 17 alineatul (3) litera (c) și alineatul (4) din Normele privind protecția datelor. O parte terță este definită la articolul 3 alineatul (1) litera (l) din Normele privind protecția datelor ca orice persoană fizică sau juridică, autoritate publică, agenție sau organism, altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal.

([99]) Articolul 17 alineatul (4) din Normele privind protecția datelor. Astfel de cerințe de confidențialitate se aplică, de exemplu, în contextul prelucrării datelor cu caracter personal ale personalului de către serviciul medical al Organizației Europene de Brevete [caz în care medicii relevanți pot fi supuși obligației de păstrare a secretului profesional – a se vedea, de exemplu, articolul 11 alineatul (3) din Normele privind protecția datelor și Normele de punere în aplicare a articolelor 83a, 84 și 84a din Statutul personalului, paragraful E] sau în contextul procedurilor de recrutare (secțiunea 6 din anexa II – Proceduri de concurs pentru posturi pentru care președintele este autoritatea împuternicită să facă numiri).

([100]) Cu alte cuvinte, atunci când CBE sau instrumentele juridice adoptate în temeiul său reglementează în mod specific informațiile care trebuie divulgate persoanelor fizice sau publicului – a se vedea informații mai detaliate în secțiunea 1.4.6.7 de mai jos.

([101]) Articolul 15 alineatul (1) din Normele privind protecția datelor.

([102]) Articolul 15 alineatul (2) din Normele privind protecția datelor.

([103]) Articolul 15 alineatul (4) din Normele privind protecția datelor. În plus, articolul 13 alineatul (2) din Normele privind protecția datelor precizează în mod clar că, în cazul în care operatorul poate demonstra că nu este în măsură să identifice persoana vizată, dispozițiile privind drepturile individuale nu se aplică (cu excepția cazului în care persoana vizată furnizează informații suplimentare care permit identificarea sa).

([104]) Articolul 15 alineatul (3) din Normele privind protecția datelor.

(45) În primul rând, în ceea ce privește dreptul de acces, Normele privind protecția datelor oferă persoanelor fizice dreptul de a obține din partea Organizației Europene de Brevete confirmarea sau infirmarea prelucrării datelor cu caracter personal care le privesc și, în caz afirmativ, de a accesa datele cu caracter personal cu ușurință ([105]) și la intervale rezonabile ([106]). În plus, persoanele fizice au dreptul de a obține informații, în special cu privire la scopul prelucrării, la categoriile de date vizate, la destinatarii cu care sunt partajate datele și la perioada preconizată pentru care vor fi stocate datele ([107]).

(46) În al doilea rând, Normele privind protecția datelor prevede că dreptul la rectificare prevăzut de acestea permite persoanelor fizice să obțină rectificarea datelor inexacte sau completarea datelor incomplete (de exemplu prin furnizarea unei declarații suplimentare) ([108]). Odată ce are loc rectificarea, operatorul are obligația de a o comunica fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal ([109]). În temeiul Normelor privind protecția datelor, dreptul la rectificare se aplică datelor obiective și factuale și nu declarațiilor subiective ([110]), deși, în acest caz, persoanelor fizice li se permite să completeze datele existente cu o a doua opinie sau cu o contraexpertiză sau să prezinte observații ([111]).

(47) În al treilea rând, Normele privind protecția datelor oferă, de asemenea, persoanelor fizice dreptul la ștergerea datelor ([112]), în special în cazul în care (a) datele cu caracter personal nu mai sunt necesare în scopul în care sunt prelucrate, (b) persoana vizată își retrage consimțământul și nu există niciun alt temei juridic pentru prelucrare, (c) persoana vizată se opune prelucrării și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea, (d) datele au fost prelucrate în mod ilegal (e) sau datele trebuie șterse pentru a respecta o obligație legală care se aplică operatorului ([113]). Operatorul trebuie să comunice orice ștergere fiecărui destinatar cu care au fost partajate datele, cu excepția cazului în care acest lucru se dovedește imposibil sau implică eforturi disproporționate ([114]). În mod similar, în cazul în care operatorul a făcut publice datele cu caracter personal, acesta trebuie să ia măsuri rezonabile pentru a informa alți operatori care le prelucrează că persoana fizică respectivă a solicitat ștergerea lor ([115]). Dreptul la ștergerea datelor nu se aplică în următoarele scenarii, în măsura în care prelucrarea datelor este necesară (a) pentru exercitarea dreptului la libertatea de exprimare și de informare, (b) pentru respectarea unei obligații legale a Organizației Europene de Brevete sau a unei obligații care decurge din obligația Organizației Europene de Brevete de a coopera cu statele sale contractante ([116]) sau pentru exercitarea autorității publice cu care este învestită Organizația Europeană de Brevete ([117]), (c) din motive de cooperare cu statele contractante în domeniul sănătății publice ([118]), (d) în scopuri de arhivare, de cercetare științifică sau istorică și în scopuri statistice (în măsura în care ștergerea ar putea face imposibilă sau ar afecta grav realizarea obiectivelor prelucrării) sau (e) pentru constatarea, exercitarea sau apărarea unui drept în instanță ([119]).

([105]) În special, operatorul trebuie să furnizeze o copie, într-o formă inteligibilă, a datelor care fac obiectul prelucrării și a tuturor informațiilor disponibile [de orice tip, indiferent de natura lor (obiectivă sau subiectivă), de conținut (inclusiv orice tip de activitate desfășurată) sau de format (dosar pe suport de hârtie, evidențe electronice, e-mailuri)] – a se vedea articolul 18 alineatul (3) din Normele privind protecția datelor. În același timp, dreptul de a obține o copie a datelor nu poate aduce atingere drepturilor și libertăților altora [articolul 18 alineatul (5) din Normele privind protecția datelor].

([106]) Articolul 18 alineatul (1) din Normele privind protecția datelor.

([107]) Articolul 18 alineatele (2)-(3) din Normele privind protecția datelor.

([108]) Articolul 19 alineatul (1) din Normele privind protecția datelor.

([109]) Articolul 19 alineatul (3) din Normele privind protecția datelor. În cazul în care persoana vizată solicită acest lucru, operatorul trebuie să furnizeze informații cu privire la destinatarii respectivi.

([110]) Această interpretare a fost adoptată în conformitate cu orientările emise de AEPD referitoare la drepturile persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal – https://www.edps.europa.eu/sites/default/files/publication/14-02-25_gl_ds_rights_en.pdf. A se vedea în special, p. 18, care conține orientări referitoare la dreptul la rectificare, cu trimiteri la „date obiective și factuale” și la „declarații subiective”.

([111]) Articolul 19 alineatul (2) din Normele privind protecția datelor.

([112]) Ștergerea datelor este definită ca „ștergerea datelor stocate astfel încât să nu fie posibilă reconstituirea lor” [articolul 3 alineatul (1) litera (v) din Normele privind protecția datelor]. Trimiterea la „datele stocate” se referă la toate datele colectate și deținute de operator (și de orice parte terță în numele operatorului).

([113]) Articolul 20 alineatul (1) din Normele privind protecția datelor.

([114]) Articolul 20 alineatul (4) din Normele privind protecția datelor.

([115]) Articolul 20 alineatul (2) din Normele privind protecția datelor.

([116]) În temeiul articolului 20 din Protocolul Organizației Europene de Brevete cu privire la privilegii și imunități, Organizația Europeană de Brevete poate fi obligată să furnizeze date cu caracter personal statelor sale contractante în contextul unor proceduri administrative sau judiciare, de exemplu pentru calcularea și transferul drepturilor de pensie ale personalului, pentru investigații fiscale sau în contextul proceselor civile privind personalul Organizației Europene de Brevete.

([117]) Aceasta se referă la situațiile în care Organizația Europeană de Brevete este obligată în temeiul CBE, al Tratatului de cooperare în domeniul brevetelor sau al instrumentelor juridice adoptate pe această bază să prelucreze date cu caracter personal în legătură cu procedura de acordare a brevetelor (de exemplu păstrarea informațiilor în Registrul european de brevete și în Buletinul european de brevete în temeiul articolelor 127 și 129 din CBE).

([118]) Prelucrarea datelor privind sănătatea din motive de interes public în domeniul sănătății publice trebuie să se realizeze în conformitate cu articolul 11 alineatul (2) litera (g) din Normele privind protecția datelor.

([119]) Articolul 20 alineatul (3) din Normele privind protecția datelor.

(48) În al patrulea rând, articolul 21 din Normele privind protecția datelor prevede un drept la restricționarea prelucrării, și anume marcarea datelor cu caracter personal cu scopul de a limita prelucrarea acestora în viitor (inclusiv măsuri de programare pentru a împiedica permanent accesul la astfel de date) ([120]). Acest drept poate fi invocat în special în cazul în care exactitatea datelor cu caracter personal este contestată de persoana fizică în cauză (pentru o perioadă de timp necesară operatorului pentru a verifica exactitatea datelor) sau în cazul în care prelucrarea este ilegală, dar persoana fizică respectivă se opune ștergerii datelor ([121]). În cazul în care prelucrarea este restricționată, datele cu caracter personal pot fi prelucrate, cu excepția stocării, numai cu consimțământul explicit al persoanei fizice în cauză, pentru constatarea, exercitarea sau apărarea unui drept în instanță, pentru protecția drepturilor altora sau pentru îndeplinirea unei atribuții în exercitarea activităților oficiale ale Organizației Europene de Brevete (și anume o atribuție care este necesară pentru activitatea administrativă și tehnică pe care Organizația Europeană de Brevete trebuie să o efectueze în conformitate cu CBE) ([122]).

(49) În al cincilea rând, dreptul la opoziție este prevăzut la articolul 1B alineatul (4) din Statutul personalului și la articolul 23 din Normele privind protecția datelor. În special, persoanele fizice au dreptul de a se opune în orice moment prelucrării datelor cu caracter personal efectuate pentru îndeplinirea unei atribuții în exercitarea activităților oficiale ale Organizației Europene de Brevete sau în exercitarea legitimă a autorității publice cu care este învestit operatorul ([123]). Persoanele fizice trebuie să fie informate cu privire la existența unui astfel de drept în mod clar și cel târziu în momentul primei comunicări cu acestea ([124]). În cazul în care o persoană fizică se opune prelucrării datelor cu caracter personal, Normele privind protecția datelor impun operatorului să înceteze prelucrarea, cu excepția cazului în care operatorul este în măsură să demonstreze motive legitime imperioase pentru prelucrare care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau pentru constatarea, exercitarea sau apărarea unui drept în instanță ([125]).

(50) În al șaselea rând, Normele privind protecția datelor stabilesc un drept la portabilitatea datelor, oferind persoanelor fizice posibilitatea de a-și primi datele cu caracter personal într-un format structurat, utilizat în mod curent și care poate fi citit automat și de a transmite datele respective unui alt operator ([126]). Acest drept se aplică în cazul în care prelucrarea este efectuată prin mijloace automatizate și are loc pe baza consimțământului persoanei fizice în cauză sau pentru executarea unui contract cu persoana fizică în cauză sau în interesul acesteia ([127]).

(51) În sfârșit, în temeiul Normelor privind protecția datelor, persoanele fizice au dreptul de a nu face obiectul unui proces decizional automatizat, și anume unei decizii bazate exclusiv pe prelucrarea automată, incluzând crearea de profiluri, care produce efecte juridice care privesc persoanele fizice sau le afectează în mod similar într-o măsură semnificativă ([128]). Normele privind protecția datelor prevăd că procesul decizional automatizat poate avea loc atunci când se bazează pe consimțământul explicit al persoanei vizate sau dacă acesta este necesar pentru încheierea sau executarea unui contract cu persoana vizată, caz în care operatorul trebuie să pună în aplicare garanții adecvate, cum ar fi prin acordarea dreptului persoanelor fizice de a obține intervenție umană, de a-și exprima punctul de vedere și de a contesta decizia ([129]). Procesul decizional automatizat poate fi, de asemenea, autorizat printr-un act juridic în cazul în care actul respectiv prevede măsuri adecvate pentru protejarea drepturilor persoanelor fizice ([130]). În cazul în care operatorul derulează un proces decizional automatizat, incluzând crearea de profiluri, acesta trebuie să informeze în mod proactiv persoana fizică în cauză în acest sens, ca parte a obligațiilor sale în materie de transparență, și să furnizeze informații semnificative cu privire la logica utilizată, precum și cu privire la importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată ([131]). Aceleași informații trebuie furnizate la cerere ([132]).

([120]) Articolul 3 alineatul (1) litera (c) din Normele privind protecția datelor.
([121]) Articolul 21 alineatul (1) din Normele privind protecția datelor.
([122]) Articolul 21 alineatul (2) din Normele privind protecția datelor.
([123]) În cazul în care Organizația Europeană de Brevete are obligația legală de a prelucra date cu caracter personal în contextul procedurii de acordare a brevetelor, și anume în temeiul CBE și al Tratatului de cooperare în domeniul brevetelor, persoanele fizice nu se pot opune prelucrării – a se vedea punctul 28 din anexa la Decizia privind procedurile de acordare a brevetelor și procedurile conexe. În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare științifică sau istorică ori în scopuri statistice, persoanele vizate au dreptul de a se opune, din motive legate de situația lor particulară, prelucrării datelor cu caracter personal, cu excepția cazului în care prelucrarea este necesară pentru îndeplinirea unei atribuții în exercitarea legitimă a autorității publice cu care este învestit operatorul, care include prelucrarea necesară pentru administrarea și funcționarea Oficiului [articolul 23 alineatul (4) din Normele privind protecția datelor].
([124]) Articolul 23 alineatul (2) din Normele privind protecția datelor.
([125]) Articolul 23 alineatul (1) din Normele privind protecția datelor.
([126]) Articolul 22 alineatul (1) din Normele privind protecția datelor.
([127]) Întrucât prelucrarea datelor cu caracter personal în contextul procedurii de acordare a brevetelor nu se întemeiază pe niciunul dintre aceste motive, dreptul la portabilitatea datelor nu se aplică într-un astfel de context – a se vedea punctele 29-30 din anexa la Decizia privind procedurile de acordare a brevetelor și procedurile conexe.
([128]) Articolul 24 alineatul (1) din Normele privind protecția datelor. Crearea de profiluri este definită la articolul 3 alineatul (1) litera (d) din Normele privind protecția datelor ca însemnând orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia.
([129]) Articolul 24 alineatul (3) din Normele privind protecția datelor.
([130]) Articolul 24 alineatul (2) litera (b) din Normele privind protecția datelor.
([131]) A se vedea articolul 16 alineatul (2) litera (f) și articolul 17 alineatul (2) litera (f) din Normele privind protecția datelor.
([132]) Articolul 18 alineatul (1) litera (h) din Normele privind protecția datelor.

2.4.6.2. *Restricții privind drepturile individuale*

(52) În mod similar celor prevăzute la articolul 23 din Regulamentul (UE) 2016/679 și la articolul 25 din Regulamentul (UE) 2018/1725, articolul 25 din Normele privind protecția datelor prevede că dispozițiile legale specifice din cadrul juridic al Organizației Europene de Brevete pot restricționa aplicarea drepturilor menționate în considerentele 43-51 ([133]) (și anume pot limita temporar aplicarea acestora) ([134]), atunci când o astfel de restricție respectă esența drepturilor ([135]) și libertăților fundamentale și reprezintă o măsură necesară și proporțională într-o societate democratică pentru a proteja obiective specifice ([136]). În plus, o restricție trebuie să fie prevăzută prin dispoziții „clare și precise" care sunt destinate să producă efecte juridice față de persoanele vizate și care trebuie adoptate cel puțin la nivelul președintelui ([137]). Astfel de dispoziții trebuie, în special, să stabilească scopul prelucrării, domeniul de aplicare al restricției, garanțiile pentru prevenirea abuzurilor, precum și perioadele de stocare și garanțiile aplicabile ([138]).

(53) În prezent, singurul instrument juridic care prevede restricții privind drepturile individuale este Circulara nr. 420 (un instrument obligatoriu din punct de vedere juridic adoptat de președinte). Aceasta clarifică modul și condițiile în care pot fi aplicate restricțiile de către operator și stabilește, în mod exhaustiv, scenariile specifice în care și obiectivele pentru care pot fi restricționate drepturile ([139]). În special, aceasta prevede că Organizația Europeană de Brevete poate restricționa drepturile individuale pentru anumite obiective specifice: (a și b) atunci când desfășoară proceduri de investigare sau disciplinare în legătură cu personalul său ([140]), (c) în contextul soluționării interne a disputelor sau al constatării, exercitării sau apărării unui drept în instanță, inclusiv în contextul arbitrajului, pentru a păstra informațiile și documentele confidențiale obținute de la părți, de la intervenienți sau din alte surse legitime, (d) atunci când prelucrează date privind sănătatea în cadrul procedurilor și dosarelor medicale, însă numai pentru a proteja drepturile persoanelor fizice ([141]), (e și f) atunci când efectuează audituri și inspecții interne (acestea din urmă sunt efectuate de responsabilul cu protecția datelor), (g) în scopul gestionării incidentelor informatice și al rapoartelor privind incidentele de securitate fizică și (h) atunci când acordă asistență autorităților publice competente sau beneficiază de asistență din partea acestora, inclusiv din partea statelor contractante ale Organizației Europene de Brevete și a organizațiilor internaționale, sau atunci când cooperează cu acestea cu privire la activitățile definite în acordurile relevante privind nivelul serviciilor, memorandumurile de înțelegere și acordurile de cooperare, fie la cererea acestora, fie din propria inițiativă a Oficiului ([142]).

([133]) Cu excepția dreptului la opoziție, pentru care Circulara nr. 420 nu prevede nicio restricție – a se vedea articolul 3 alineatul (3). În plus, în temeiul articolului 9 din Circulara nr. 420, Organizația Europeană de Brevete poate restricționa informarea unei persoane cu privire la o încălcare a securității datelor.

([134]) A se vedea definiția restricțiilor de la articolul 2 din Circulara nr. 420.

([135]) Restricțiile care sunt atât de extinse și de intruzive încât, în fapt, privează un drept fundamental de substanța sa de bază și împiedică persoana fizică respectivă să îl exercite nu pot fi justificate [a se vedea articolul 4 alineatul (3) din Circulara nr. 420].

([136]) Și anume securitatea Organizației Europene de Brevete, siguranța publică sau apărarea statelor contractante, prevenirea, investigarea, depistarea și urmărirea penală a infracțiunilor sau executarea sancțiunilor penale, inclusiv protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora, alte interese fundamentale ale Organizației Europene de Brevete legate de misiunea sa principală sau ca urmare a obligațiilor care decurg din obligația de cooperare cu statele contractante, inclusiv aspecte de ordin monetar, bugetar și fiscal, precum și sănătatea publică și securitatea socială, securitatea internă a Oficiului, inclusiv a rețelelor sale de comunicații electronice, protecția independenței judiciare și cvasijudiciare și a procedurilor judiciare și cvasijudiciare, prevenirea, investigarea, depistarea și urmărirea penală a încălcării eticii în cazul profesiilor reglementate, o funcție de monitorizare, inspecție sau reglementare legată, chiar și ocazional, de exercitarea autorității publice, precum și protecția persoanei vizate sau a drepturilor și libertăților altora și punerea în aplicare a pretențiilor de drept civil [articolul 25 alineatul (1) din Normele privind protecția datelor].

([137]) Articolul 25 alineatul (3) din Normele privind protecția datelor.

([138]) Articolul 25 alineatul (2) din Normele privind protecția datelor.

([139]) Articolul 1 din Circulara nr. 420.

([140]) Articolul 4 alineatul (1) literele (a)-(b) din Circulara nr. 420.

([141]) Această situație vizează numai prelucrarea datelor privind sănătatea ale personalului Organizației Europene de Brevete (și nu este direct relevantă în scopul constatării referitoare la caracterul adecvat care vizează prelucrarea datelor transferate de la un operator sau de la o persoană împuternicită de operator care face obiectul RGPD). Articolul 8 din Circulara nr. 420 clarifică suplimentar modul în care pot fi aplicate restricțiile privind dreptul de acces la datele/dosarele medicale. În special, acesta precizează că o astfel de restricție se poate aplica numai dreptului de acces direct la datele lor medicale cu caracter personal și/sau la dosarele de natură psihologică sau psihiatrică prelucrate de Oficiu, dar numai în cazul în care accesul la aceste date este de natură să afecteze în mod negativ și să reprezinte un pericol imediat pentru viața și sănătatea persoanei vizate sau a altor persoane.

([142]) Articolul 4 alineatul (1) din Circulara nr. 420. Această dispoziție vizează, în general, numai datele cu caracter personal ale personalului Organizației Europene de Brevete. Ea se referă la cazurile în care Organizația Europeană de Brevete are obligația de a coopera cu autoritățile naționale ale statelor contractante în temeiul articolului 131 din CBE (care reglementează cooperarea dintre Organizația Europeană de Brevete și instanțele naționale ale statelor contractante în cadrul investigațiilor/procedurilor referitoare la acordarea brevetelor) și în temeiul articolului 20 alineatul (1) din Protocolul cu privire la privilegii și imunități (a se vedea, de asemenea, punctul 95). O astfel de situație poate apărea, de exemplu, în cazul în care personalului Organizației Europene de Brevete i se solicită să depună mărturie înaintea unei instanțe naționale a unui stat contractant în contextul unor proceduri penale naționale sau în care Organizației Europene de Brevete i se solicită să furnizeze informații cu privire la salariul personalului său în cadrul procedurilor civile (de drept al familiei) etc.

(54) Operatorul trebuie să stabilească dacă se poate aplica sau nu o restricție într-un caz specific în situații individuale, având în vedere circumstanțele relevante ([143]). Atunci când decide dacă să aplice sau nu o restricție, operatorul trebuie mai întâi să evalueze necesitatea și proporționalitatea acesteia în cazul specific, cu implicarea responsabilului cu protecția datelor ([144]). Această evaluare implică o punere în balanță a riscurilor potențiale pentru drepturile și libertățile persoanei vizate cu riscurile și libertățile altor persoane vizate și cu riscurile de obstrucționare a scopului și a rezultatului operațiunii de prelucrare ([145]). Restricțiile trebuie să fie documentate, inclusiv prin înregistrarea evaluării drepturilor restricționate, precum și a duratei, a motivelor și a temeiurilor acestora ([146]). În plus, atât timp cât se aplică o restricție, trebuie puse în aplicare măsuri tehnice și organizatorice adecvate ([147]). Orice restricție poate fi aplicată numai atât timp cât există motive pentru aplicarea restricției respective ([148]). În cazul restricționării unui drept, operatorul trebuie să informeze persoana fizică în cauză cu privire la principalele motive și la dreptul acesteia de a depune o plângere ([149]).

2.4.6.3. *Norme specifice în contextul procedurii de acordare a brevetelor*

(55) Dispozițiile tratatului constitutiv al Organizației Europene de Brevete (și anume CBE), ale Tratatului de cooperare în domeniul brevetelor și dispozițiile aplicabile în temeiul acestora (toate constituind legislația primară a Organizației Europene de Brevete) conțin anumite cerințe specifice, în contextul procedurii de acordare a brevetelor, care pot avea un impact asupra exercitării anumitor drepturi în temeiul Normelor privind protecția datelor ([150]). Decizia privind procedurile de acordare a brevetelor și procedurile conexe oferă o imagine de ansamblu a acestor cerințe ale legislației primare, explică modul în care pot fi exercitate drepturile persoanelor vizate în acest context și stabilește în mod clar posibilele excepții ([151]). Circulara nr. 420 stabilește că dispozițiile care pot limita aplicarea drepturilor în materie de protecție a datelor trebuie să identifice în mod clar domeniul de aplicare al oricărei excepții și, prin urmare, să echilibreze diferitele interese aflate în joc ([152]).

(56) În primul rând, în temeiul articolului 127 din CBE, Oficiul este obligat să mențină Registrul european de brevete, în care sunt publicate anumite date cu caracter personal definite de lege. În conformitate cu legislația primară, cererile de brevet trebuie publicate în cursul procedurii de acordare a brevetelor, în general, cât mai curând posibil după expirarea unui termen de optsprezece luni de la data depunerii. CBE prevede că datele cu caracter personal incluse în astfel de cereri de brevet pot fi accesate fie prin consultarea dosarului, fie prin consultarea registrului ([153]). Înainte de publicare, cererile de brevet nu sunt disponibile pentru consultare fără consimțământul explicit al solicitantului. Tratatul de cooperare în domeniul brevetelor prevede norme similare ([154]).

([143]) Articolul 2 din Circulara nr. 420.

([144]) Articolul 25 alineatul (3) litera (a) din Normele privind protecția datelor. A se vedea, de asemenea, articolul 6 din Circulara nr. 420.

([145]) Articolul 5 alineatul (5) din Circulara nr. 420.

([146]) Articolul 4 alineatul (4) din Circulara nr. 420. Aceste evidențe trebuie puse la dispoziția Comitetului pentru protecția datelor la cerere [articolul 4 alineatul (7) din Circulara nr. 420].

([147]) Măsurile trebuie să includă, de exemplu, stocarea securizată, un mediu electronic securizat care să prevină accesul ilegal și accidental la datele electronice sau transferul acestora către persoane neautorizate, precum și monitorizarea restricțiilor și revizuirea periodică a aplicării acestora – a se vedea articolul 5 alineatul (2) din Circulara nr. 420.

([148]) Articolul 4 alineatul (5) și articolul 5 alineatul (3) din Circulara nr. 420.

([149]) Articolul 25 alineatul (3) litera (b) din Normele privind protecția datelor. O astfel de informare poate fi amânată, omisă sau refuzată dacă aceasta ar urma să anuleze efectul restricției – a se vedea articolul 25 alineatul (4) din Normele privind protecția datelor. Această restricție suplimentară poate fi aplicată numai în cazuri justificate în mod corespunzător și atât timp cât și în măsura în care este necesară și proporțională [articolul 7 alineatul (4) din Circulara nr. 420]. Justificarea unei astfel de restricții trebuie reevaluată periodic. Pe lângă cerința specifică de informare a persoanelor fizice cu privire la o restricționare a drepturilor lor, Organizația Europeană de Brevete trebuie să furnizeze informații generale pe intranetul său și/sau pe site-ul său web cu privire la activitățile care pot implica restricții ale drepturilor [articolul 7 alineatul (1) din Circulara nr. 420].

([150]) Articolul 2 din Circulara nr. 420 (dispoziții legale ale Organizației Europene de Brevete).

([151]) Articolul 1 și anexa la Decizia privind procedurile de acordare a brevetelor și procedurile conexe.

([152]) Articolul 2 din Circulara nr. 420.

([153]) Punctele C.13 și C.14 din anexa la Decizia privind procedurile de acordare a brevetelor și procedurile conexe și articolul 128 din CBE. Anumite părți ale dosarelor sunt excluse de la consultare în conformitate cu articolul 128 alineatul (4) și cu norma 144 din Regulamentul de punere în aplicare a CBE, precum și cu Decizia președintelui OEB din 12.7.2007 privind documentele excluse de la consultarea dosarelor (ediția specială nr. 3, JO OEB 2007, J.3). Părțile excluse sunt următoarele: documentele referitoare la excluderea membrilor camerelor de recurs sau ai Marii Camere de Apel sau la obiecțiile ridicate în legătură cu aceștia, proiectele de decizii și notificări, precum și toate celelalte documente utilizate pentru elaborarea deciziilor și a notificărilor, care nu sunt comunicate părților, mențiunea cu privire la inventator, în cazul în care acesta a renunțat la dreptul său de a fi menționat și orice alt document exclus de la consultare de către președintele Oficiului European de Brevete pe motiv că o astfel de consultare nu ar servi scopului de a informa publicul cu privire la cererea de brevet european sau la brevetul european, cum ar fi: certificatele medicale, cererile de excludere de la consultarea dosarelor și corespondența aferentă, precum și informațiile a căror publicare ar aduce atingere intereselor legitime personale sau economice și nu ar cuprinde informații relevante pentru cererea sau pentru brevetul în cauză ori pentru procedura de acordare a brevetelor.

([154]) A se vedea articolul 3 din Decizia președintelui OEB din 20.2.2019 privind consultarea online a documentelor conținute în dosarul deținut de OEB în calitate de oficiu de primire, autoritate internațională de cercetare sau autoritate specificată pentru cercetare suplimentară (JO, Oficiul European de Brevete, 2019, A17). A se vedea în acest sens articolul 30 din Tratatul de cooperare în domeniul brevetelor în ceea ce privește accesul public la dosare, precum și normele 94 și 48 din Tratatul de cooperare în domeniul brevetelor. Dispozițiile respective sunt utilizate de Organizația Europeană de Brevete atunci când aceasta acționează în calitate de oficiu sau autoritate competentă în temeiul Tratatului de cooperare în domeniul brevetelor în conformitate cu articolele 151-153 din CBE.

(57) În al doilea rând, posibilitatea de a obține modificări ale informațiilor utilizate în cadrul unei proceduri de acordare a brevetelor este reglementată în mod specific de CBE ([155]). În special, CBE prevede doar posibilitatea de a obține corectarea erorilor din documentele depuse la Organizația Europeană de Brevete ([156]), corectarea erorilor din decizii ([157]), corectarea traducerilor ([158]) și rectificarea mențiunii cu privire la inventator ([159]). Prin urmare, rectificarea datelor cu caracter personal incluse în documentele utilizate în procedura de acordare a brevetelor nu poate fi obținută decât în aceste cazuri. Același lucru este valabil și pentru posibilitatea de a obține o restricționare a prelucrării datelor ([160]).

(58) În al treilea rând, CBE impune cerințe specifice de păstrare și de publicare pentru anumite documente utilizate în procedura de acordare a brevetelor, care au un impact asupra posibilității de a obține ștergerea informațiilor conținute în acestea, inclusiv a datelor cu caracter personal ([161]). În special, cererile de brevete publicate și informațiile privind brevetele publicate în Buletinul european de brevete trebuie păstrate și puse la dispoziția publicului ([162]). În consecință, ștergerea datelor cu caracter personal conținute în aceste documente ar contraveni obligațiilor juridice fundamentale ale Organizației Europene de Brevete [articolul 129 litera (a) din CBE] și nu poate fi obținută. Alte dosare trebuie păstrate de Organizația Europeană de Brevete pentru o perioadă specificată în CBE, care este, în principiu, de cinci ani ([163]). Atât timp cât se aplică această perioadă, nu se poate obține ștergerea informațiilor conținute în aceste dosare (inclusiv a datelor cu caracter personal).

(59) Prin urmare, ținând seama în special de domeniul și de condițiile lor limitate de aplicare, restricțiile privind exercitarea drepturilor care decurg din dispozițiile menționate în considerentele 55-58 pot fi considerate ca fiind limitate la ceea ce este necesar și proporțional pentru a asigura funcționarea corectă a procedurii de acordare a brevetelor, astfel cum este necesar în interesul public pentru îndeplinirea atribuțiilor oficiale ale Organizației Europene de Brevete. În măsura în care CBE și Tratatul de cooperare în domeniul brevetelor nu reglementează în mod specific exercitarea drepturilor în materie de protecție a datelor, și anume în toate celelalte scenarii decât cele descrise în considerentele 55-58, cerințele din Normele privind protecția datelor se aplică integral.

2.4.7. ***Transferuri ulterioare***

(60) Nivelul de protecție conferit datelor cu caracter personal transferate din Uniune către Organizația Europeană de Brevete nu trebuie să fie diminuat de transferul ulterior al acestor date către destinatari dintr-o țară terță sau o altă organizație internațională.

(61) Normele privind protecția datelor fac distincție între „transmiterile de date cu caracter personal” (și anume schimbul de date dintre Organizația Europeană de Brevete și statele sale contractante) și „transferurile de date cu caracter personal” (schimbul de date dintre Organizația Europeană de Brevete și orice altă persoană sau entitate din afara Organizației Europene de Brevete) ([164]).

2.4.7.1. *Transmiterile de date*

(62) În primul rând, Normele privind protecția datelor prevăd că o transmitere de date către un oficiu național pentru proprietate intelectuală al unui stat contractant al Organizației Europene de Brevete poate avea loc în cazul în care datele sunt necesare pentru (a) îndeplinirea competenței destinatarului sau exercitarea autorității publice și (b) transmiterea este necesară pentru exercitarea atribuțiilor/autorității publice a Organizației Europene de Brevete ([165]). Aceste transmiteri au loc în contextul procedurii de acordare a brevetelor prevăzute de CBE și de Tratatul de cooperare în domeniul brevetelor ([166]).

([155]) O corectare sau o rectificare în temeiul acestor dispoziții poate duce la actualizarea înregistrărilor din Registrul european de brevete și din Buletinul european de brevete, precum și a informațiilor publicate cu privire la cerere sau la brevet. Cu toate acestea, ea nu va modifica retroactiv conținutul dosarului (care va continua să conțină toate observațiile părților și toate comunicările și deciziile Organizației Europene de Brevete). Aceasta nu va conduce nici la retragerea sau eliminarea informațiilor publicate anterior (punctul C.19 din anexa la Decizia privind procedura de acordare a brevetelor și procedurile conexe). Acest lucru se aplică, de asemenea, în temeiul articolelor 19 și 34 din Tratatul de cooperare în domeniul brevetelor, atunci când Organizația Europeană de Brevete acționează în calitate de autoritate/oficiu competent în temeiul articolului 151-153 din CBE.

([156]) Norma 139 din Regulamentul de punere în aplicare a CBE.

([157]) Norma 140 din Regulamentul de punere în aplicare a CBE. În cuprinsul deciziilor Organizației Europene de Brevete, se pot modifica numai greșelile de ortografie, greșelile de transcriere și erorile evidente.

([158]) Articolul 14 alineatul (2) a doua teză din CBE.

([159]) Norma 21 din Regulamentul de punere în aplicare a CBE. O mențiune incorectă cu privire la un inventator poate fi rectificată la cerere și numai cu consimțământul persoanei menționate în mod eronat și, în cazul în care o astfel de cerere este depusă de o parte terță, cu consimțământul solicitantului sau al titularului brevetului.

([160]) Punctul C.25 din anexa la Decizia privind procedura de acordare a brevetelor și procedurile conexe.

([161]) Punctele C.22-C.23 din anexa la Decizia privind procedurile de acordare a brevetelor și procedurile conexe.

([162]) Articolul 129 din CBE.

([163]) Norma 147 alineatele (4) și (5) din Regulamentul de punere în aplicare a CBE.

([164]) Articolul 3 alineatul (1) literele (s) și (t) din Normele privind protecția datelor.

([165]) Articolul 8 alineatul (2) din Normele privind protecția datelor.

([166]) A se vedea, în special, articolele 130, 131 și 135 din CBE, precum și Regulamentul de punere în aplicare relevant în temeiul CBE (de exemplu, normele 148-150). A se vedea, de asemenea, articolele 12, 18, 20 și 36 din Tratatul de cooperare în domeniul brevetelor, precum și normele 22, 23, 23 bis, 44, 47 și 71 din Regulamentul de punere în aplicare.

(63) În al doilea rând, Normele privind protecția datelor permit o transmitere de date către o autoritate publică a unui stat contractant al Organizației Europene de Brevete ([167]), în cazul în care datele sunt necesare pentru îndeplinirea atribuțiilor autorității publice respective, iar transmiterea lor este compatibilă cu atribuțiile și cu funcționarea Organizației Europene de Brevete ([168]). Astfel de transmiteri de date nu sunt solicitate în mod specific în temeiul CBE sau al altor instrumente juridice care reglementează procedura de acordare a brevetelor, dar pot fi totuși necesare pentru îndeplinirea atribuțiilor Organizației Europene de Brevete, de exemplu cooperarea Organizației Europene de Brevete cu statele sale contractante prin intermediul proceselor de consultare, detașarea și delegarea de experți sau furnizarea de informații cu privire la personalul Organizației Europene de Brevete în scopul stabilirii prestațiilor sociale sau în legătură cu cerințele fiscale etc.

(64) Responsabilul cu protecția datelor a elaborat clauze standard care să fie incluse în memorandumurile de înțelegere pentru reglementarea unor astfel de transmiteri descrise la considerentele 62 și 63, care, printre altele, prevăd principii de protecție a datelor, limitează prelucrarea ulterioară numai în scopuri compatibile, prevăd drepturi ale persoanelor vizate, precum și obligații în ceea ce privește securitatea datelor și încălcarea securității datelor, precum și supravegherea independentă ([169]).

(65) În ambele scenarii descrise în considerentele 62 și 63, destinatarul, în temeiul Normelor privind protecția datelor, trebuie să furnizeze dovezi că este necesar ca datele să fie transmise pentru un scop specific care decurge din obligațiile Organizației Europene de Brevete de cooperare cu statul sau statele contractante ([170]). Operatorul trebuie să fie în măsură, pentru fiecare transmitere de date, să demonstreze că o astfel de transmitere este necesară și proporțională cu scopul specific pentru care se realizează partajarea ([171]). Orice transmitere de date trebuie efectuată într-un mod care să asigure menținerea nivelului de protecție oferit de Normele privind protecția datelor ([172]). Potrivit orientărilor emise de responsabilul cu protecția datelor, aceasta înseamnă că sunt instituite garanții adecvate, inclusiv prin asigurarea faptului că datele care urmează să fie partajate trebuie reduse la minimum și limitate la ceea ce este adecvat, relevant și strict necesar pentru atingerea scopului respectiv ([173]). În cazul în care există orice motiv să se presupună că interesele legitime ale persoanei în cauză pot fi afectate, operatorul trebuie să stabilească faptul că transmiterea datelor cu caracter personal în acest scop specific este proporțională, după punerea în balanță a diferitelor interese aflate în joc ([174]).

(66) În ceea ce privește aceste două scenarii, este important de remarcat, de asemenea, că toate statele contractante ale Organizației Europene de Brevete sunt părți la Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale, se supun jurisdicției Curții Europene a Drepturilor Omului și sunt părți la Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (ETS nr. 108).

(67) În sfârșit, Normele privind protecția datelor permit transmiterea datelor către o persoană împuternicită de operator situată în Spațiul Economic European (SEE), cu condiția să se asigure conformitatea cu cerințele prevăzute în Normele privind protecția datelor pentru angajarea persoanelor împuternicite de operatori ([175]).

2.4.7.2. *Transferul de date*

(68) Schimbul de date cu caracter personal cu orice entitate din afara Organizației Europene de Brevete, alta decât o autoritate publică sau un oficiu național pentru proprietate intelectuală din statele contractante ale Organizației Europene de Brevete sau o persoană împuternicită de operator din SEE, este considerată un „transfer" de date cu caracter personal, sub rezerva cerințelor specifice prevăzute în Normele privind protecția datelor ([176]). Aceste cerințe se aplică, de exemplu, schimbului de date cu persoanele împuternicite de operatori din afara SEE, cu operatorii situați

([167]) De exemplu, o autoritate națională sau locală, precum și un alt organism de drept public, cum ar fi un spital sau o universitate.
([168]) Articolul 8 alineatul (1) din Normele privind protecția datelor.
([169]) Prezentare generală a cerinței privind clauza standard de protecție a datelor a Organizației Europene de Brevete pentru memorandumurile de înțelegere, disponibilă la adresa https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-template-data-protection-clause-for-mous.pdf.
([170]) Articolul 8 alineatul (3) din Normele privind protecția datelor.
([171]) Articolul 8 alineatul (4) din Normele privind protecția datelor.
([172]) Nota explicativă intitulată „*EPO transmission and transfer of personal data*" (Transmiterea și transferul de date la nivelul Organizației Europene de Brevete) (Nota de transmitere și transfer), disponibilă la adresa https://link.epo.org/web/office/data-protection-and-privacy/en-explanatory-note-on-epo-transmission-and-transfer-of-personal-data.pdf, nota de subsol 4. A se vedea, în special, „Normele privind protecția datelor ale Organizației Europene de Brevete […] stabilește principiul general al protecției adecvate, aplicabil în special fluxului internațional de date".
([173]) Nota de transmitere și transfer, disponibilă la nota de subsol 12.
([174]) Articolul 8 alineatul (3) din Normele privind protecția datelor.
([175]) Articolul 8 alineatele (1), (2) și (5) din Normele privind protecția datelor.
([176]) Articolul 9 alineatul (1) din Normele privind protecția datelor.

în statele contractante sau în afara acestora, cu autoritățile publice din statele necontractante și cu alte organizații internaționale. În general, Normele privind protecția datelor prevăd că nivelul de protecție garantat persoanelor fizice de către Organizația Europeană de Brevete nu trebuie să fie diminuat atunci când datele sunt transferate unor părți terțe ([177]). Potrivit orientărilor responsabilului cu protecția datelor, „protecția acordată datelor cu caracter personal transferate în țara terță sau către organizația internațională în cauză trebuie să fie în esență echivalentă cu cea garantată în Normele privind protecția datelor" ([178]).

(69) În temeiul Normelor privind protecția datelor, un transfer de date cu caracter personal în afara Organizației Europene de Brevete poate avea loc în primul rând dacă țara în care se află destinatarul sau organizația internațională asigură un nivel de protecție adecvat și dacă transferul este efectuat exclusiv pentru a permite Organizației Europene de Brevete să îndeplinească atribuții care intră în sfera sa de competență ([179]). Președintele ([180]) adoptă o decizie privind caracterul adecvat al nivelului de protecție și, în cazul în care există dubii în această privință, ia decizia după consultarea responsabilului cu protecția datelor și a Comitetului pentru protecția datelor ([181]). Responsabilul cu protecția datelor a elaborat „criterii de referință privind caracterul adecvat al nivelului de protecție", prin care se stabilesc criteriile pentru deciziile privind caracterul adecvat al nivelului de protecție ([182]). În principal, cadrul juridic al țării terțe sau al organizației internaționale trebuie să prevadă, în special, principii-cheie privind protecția datelor, drepturile persoanelor vizate, norme privind transferurile ulterioare, mecanisme procedurale și de asigurare a respectării legii, precum și reparațiile disponibile pentru persoanele fizice. În cazul în care președintele adoptă o decizie privind caracterul adecvat al nivelului de protecție, transferul poate avea loc fără punerea în aplicare a unor garanții suplimentare ([183]). În prezent, Organizația Europeană de Brevete consideră că statele membre, precum și Norvegia, Islanda și Liechtenstein, toate fiind țări care beneficiază de o decizie privind caracterul adecvat al nivelului de protecție din partea Comisiei ([184]), și instituțiile și organele Uniunii oferă un nivel de protecție adecvat ([185]).

(70) În temeiul Normelor privind protecția datelor, în absența unei decizii privind caracterul adecvat al nivelului de protecție, operatorul sau persoana împuternicită de operator poate transfera date cu caracter personal către destinatari din afara Organizației Europene de Brevete numai dacă operatorul sau persoana împuternicită de operator a oferit garanții adecvate și cu condiția să existe drepturi executorii ale persoanelor vizate și căi de atac eficiente pentru persoanele vizate ([186]). Astfel de garanții adecvate pot fi incluse în acordurile administrative cu autoritățile publice sau cu organizațiile internaționale, în clauzele contractuale (după consultarea Comitetului pentru protecția datelor) ([187]) sau în mecanismele de certificare ([188]). Responsabilul cu protecția datelor a elaborat o prezentare generală a dispozițiilor care trebuie incluse în acordurile administrative ([189]). De asemenea, este disponibil un model de acord privind protecția datelor pentru transferurile către persoanele împuternicite de operatori ([190]). În conformitate cu orientările responsabilului cu protecția datelor, Organizația Europeană de Brevete trebuie să evalueze dacă importatorul de date ar fi împiedicat să își respecte obligațiile care îi revin în temeiul unui instrument de transfer din cauza cadrului juridic căruia îi este supus și, dacă este necesar, să pună în aplicare măsuri suplimentare ([191]). Pentru a efectua această evaluare, responsabilul cu protecția datelor recomandă, în notele explicative ale Organizației Europene de Brevete privind transmiterea și transferul de date cu caracter personal, să se țină seama de orientările relevante ale CEPD și ale Autorității Europene pentru Protecția Datelor ([192]).

(71) În temeiul Normelor privind protecția datelor, pentru transferurile de date către țări sau organizații care beneficiază de o decizie privind caracterul adecvat al nivelului de protecție, precum și pentru transferurile de date pe baza unor garanții adecvate, Organizația Europeană de Brevete trebuie să demonstreze necesitatea și proporționalitatea fiecărui transfer în scopul prelucrării ([193]). În plus, Organizația Europeană de Brevete trebuie să stabilească, după punerea în

([177]) Articolul 9 alineatul (1) din Normele privind protecția datelor.
([178]) Nota de transmitere și transfer, p. 11 și nota de subsol 8. „Țara terță" este definită de Normele privind protecția datelor ca o țară care nu este stat contractant la CBE – a se vedea articolul 3 alineatul (1) litera (u) din Normele privind protecția datelor.
([179]) Articolul 9 alineatul (2) din Normele privind protecția datelor.
([180]) A se vedea articolul 1 alineatul (2) litera (a) din Normele privind protecția datelor, coroborat cu articolul 10 alineatul (2) litera (a) din CBE și cu articolul 9 alineatul (2) din Normele privind protecția datelor.
([181]) Articolul 9 alineatul (3) din Normele privind protecția datelor.
([182]) Prezentare generală a criteriilor de referință privind caracterul adecvat al nivelului de protecția ale Organizației Europene de Brevete, disponibile la adresa https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-adequacy-referential-methodology.pdf.
([183]) Nota de subsol 49 din Nota de transmitere și transfer.
([184]) Cu excepția Cadrului UE-SUA privind confidențialitatea datelor.
([185]) A se vedea Decizia președintelui Oficiului European de Brevete din 17 noiembrie 2022 privind țările și entitățile despre care se consideră că asigură o protecție adecvată a datelor cu caracter personal, disponibilă la adresa https://www.epo.org/en/legal/official-journal/2022/12/a111.html.
([186]) Articolul 9 alineatele (4) și (5) din Normele privind protecția datelor.
([187]) În acest sens, orientările responsabilului cu protecția datelor se referă la clauzele contractuale standard adoptate de Comisia Europeană ca oferind o bună imagine de ansamblu a garanțiilor care trebuie incluse – a se vedea Nota de transmitere și transfer, p. 8.
([188]) Articolul 9 alineatul (5) din Normele privind protecția datelor. A se vedea, de asemenea, Nota de transmitere și transfer, p. 8.
([189]) Prezentare generală a cerințelor din modelele de acorduri administrative ale Organizației Europene de Brevete, disponibilă la adresa https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-epo's-administrative-arrangements-modules.pdf.
([190]) A se vedea Anexa E la condițiile contractuale generale pentru Organizația Europeană de Brevete, disponibilă la adresa https://link.epo.org/web/general_conditions_of_contract_en.pdf.
([191]) Nota de transmitere și transfer, p. 9.
([192]) Nota de transmitere și transfer, p. 9.
([193]) Articolul 9 alineatul (6) din Normele privind protecția datelor. În cazul în care există motive să se presupună că interesul legitim al persoanei vizate ar putea fi prejudiciat, operatorul trebuie să stabilească faptul că transferul în acest scop specific este proporțional, după punerea în balanță a diferitelor interese concurente.

balanță a diferitelor interese aflate în joc, dacă transferul este proporțional, în cazul în care există motive să se creadă că interesele legitime ale persoanelor vizate ar putea fi prejudiciate ([194]). De asemenea, trebuie să se asigure (prin garanții contractuale) faptul că destinatarul poate prelucra sau utiliza datele numai în scopurile pentru care au fost transferate, având obligația de a șterge datele de îndată ce scopul urmărit a fost atins ([195]).

(72) În temeiul Normelor privind protecția datelor, în absența unei decizii privind caracterul adecvat al nivelului de protecție sau a unor garanții adecvate, transferul de date cu caracter personal în afara Organizației Europene de Brevete este permis „numai în mod excepțional", dacă se aplică o așa-numită „derogare" în condiții similare celor prevăzute în dispozițiile corespunzătoare din legislația Uniunii privind protecția datelor ([196]). Acest lucru este valabil atunci când (a) persoana vizată și-a dat consimțământul explicit pentru transfer ([197]), (b și c) transferul este ocazional și necesar pentru executarea unui contract cu persoana vizată sau în interesul persoanei vizate (sau pentru aplicarea unor măsuri precontractuale la cererea persoanei vizate) ([198]), (d) transferul este necesar pentru îndeplinirea unei atribuții în exercitarea activităților oficiale ale Organizației Europene de Brevete sau în exercitarea legitimă a autorității publice cu care este învestit operatorul ([199]), (e) transferul este ocazional și necesar pentru constatarea, exercitarea sau apărarea unui drept în instanță ([200]), (f) transferul este necesar pentru protejarea intereselor vitale ale unei persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul ([201]) sau (g) transferul este efectuat dintr-un registru care are rolul de a oferi informații publicului și care este deschis spre consultare fie publicului în general, fie oricărei persoane care justifică un interes legitim, în măsura în care condițiile stabilite pentru o astfel de consultare sunt îndeplinite pentru fiecare caz în parte ([202]). Prin natura lor și în conformitate cu orientările responsabilului cu protecția datelor, aceste derogări nu pot fi invocate pentru transferuri sistematice și regulate ([203]).

(73) În sfârșit, în ceea ce privește transferurile unor categorii specifice de date către țări sau organizații care nu beneficiază de o decizie privind caracterul adecvat al nivelului de protecție, președintele poate limita și mai mult astfel de transferuri din motive importante legate de exercitarea legitimă a autorității publice cu care este învestit Oficiul ([204]). Până în prezent, președintele nu a făcut uz de aceste competențe.

2.4.8. ***Responsabilitate***

(74) Conform principiului responsabilității, entităților care prelucrează date li se solicită să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a-și respecta în mod efectiv obligațiile în materie de protecție a datelor și pentru a putea demonstra această conformitate, în special autorității de supraveghere competente.

(75) Articolul 4 alineatul (1) din Normele privind protecția datelor stabilește un principiu general al responsabilității, precizând în mod clar că operatorul este responsabil pentru respectarea Normelor privind protecția datelor și trebuie să fie în măsură să demonstreze respectarea acestuia. În special, operatorul trebuie să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura și a fi în măsură să demonstreze conformitatea, ținând seama de natura,

([194]) Articolul 9 alineatul (6) din Normele privind protecția datelor.
([195]) Articolul 9 alineatul (6) din Normele privind protecția datelor.
([196]) A se vedea articolul 10 din Normele privind protecția datelor, precum și nota de transmitere și transfer, p. 9-11.
([197]) Articolul 10 alineatul (1) litera (a) din Normele privind protecția datelor. În acest caz, persoana fizică în cauză trebuie să fie informată cu privire la posibilele riscuri cauzate de absența unui nivel de protecție adecvat și a unor garanții adecvate. Această derogare nu poate fi invocată de Organizația Europeană de Brevete în exercitarea activităților sale oficiale [articolul 10 alineatul (2) din Normele privind protecția datelor].
([198]) Articolul 10 alineatul (1) literele (b)-(c) și alineatul (2) din Normele privind protecția datelor. Aceste derogări nu pot fi invocate de Organizația Europeană de Brevete în exercitarea activităților sale oficiale [articolul 10 alineatul (2) din Normele privind protecția datelor].
([199]) Articolul 10 alineatul (1) litera (d) din Normele privind protecția datelor. Astfel de activități oficiale sau o astfel de autoritate publică trebuie să fie stabilite pe baza CBE sau a altor dispoziții legale aplicabile ale Organizației Europene de Brevete [articolul 10 alineatul (4) din Normele privind protecția datelor]. Aceasta include prelucrarea necesară pentru administrarea și funcționarea Oficiului sau pentru îndeplinirea obligațiilor care decurg din obligația de cooperare a Organizației Europene de Brevete cu statele contractante. Transferurile pot avea loc, de pildă, pentru îndeplinirea obligațiilor, de exemplu între Oficiu și organismele naționale, administrațiile fiscale sau vamale, autoritățile de supraveghere financiară și serviciile competente în materie de securitate socială sau de sănătate publică, de exemplu în cazul depistării punctelor de contact pentru bolile contagioase [articolul 10 alineatul (6) din Normele privind protecția datelor].
([200]) Articolul 10 alineatul (1) litera (e) și alineatul (2) din Normele privind protecția datelor.
([201]) Articolul 10 alineatul (1) litera (f) din Normele privind protecția datelor.
([202]) Articolul 10 alineatul (1) litera (g) din Normele privind protecția datelor. Un astfel de transfer nu ar trebui să implice totalitatea datelor cu caracter personal sau ansamblul categoriilor de date conținute în registru, cu excepția cazului în care este autorizat de dispozițiile legale ale Organizației Europene de Brevete, iar atunci când registrul este destinat să fie consultat de persoane care au un interes legitim, transferul ar trebui să fie efectuat doar la cererea persoanelor respective sau dacă acestea sunt destinatarii, luând pe deplin în considerare interesele și drepturile fundamentale ale persoanei vizate [articolul 10 alineatele (2) și (5) din Normele privind protecția datelor].
([203]) Nota de transmitere și transfer, p. 10.
([204]) Care, după cum s-a menționat anterior, include prelucrarea necesară pentru administrarea și funcționarea sa sau în temeiul obligațiilor care decurg din obligația sa de cooperare cu statele contractante. A se vedea articolul 10 alineatul (6) din Normele privind protecția datelor.

domeniul de aplicare, contextul și scopurile prelucrării, precum și de diferitele grade de probabilitate și gravitate ale oricăror riscuri pentru drepturile persoanelor fizice ([205]). În acest sens, Normele privind protecția datelor pun în aplicare, de asemenea, principiul protejării vieții private din faza de proiectare și al protejării implicite a vieții private, prevăzând că operatorul trebuie să pună în aplicare măsuri menite să aplice principiile de protecție a datelor și să asigure conformitatea cu Normele privind protecția datelor, precum și să se asigure că, în mod implicit, sunt prelucrate numai datele cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării ([206]).

(76) Operatorul și persoanele împuternicite de operator trebuie să păstreze o evidență a activităților de prelucrare, care să conțină, printre altele, informații privind scopul prelucrării, categoriile de date prelucrate, categoriile de destinatari cărora le sunt divulgate datele și orice transfer de date cu caracter personal ([207]). Aceste evidențe sunt, în principiu, accesibile publicului (cu excepția cazului în care conțin informații confidențiale) și sunt incluse într-un registru de protecție a datelor accesibil publicului, trebuind puse, la cerere, la dispoziția Comitetului pentru protecția datelor ([208]). Fiecare unitate operațională trebuie, de asemenea, să numească cel puțin o persoană de legătură pentru protecția datelor (cu un mandat reînnoibil de unul până la trei ani), care trebuie să urmeze o formare obligatorie în domeniul protecției datelor și să asiste operatorul în îndeplinirea obligațiilor care îi revin ([209]).

(77) În sfârșit, Normele privind protecția datelor oferă diferite instrumente care pot sprijini operatorul și persoanele împuternicite de operatori în eforturile lor de asigurare a conformității. De exemplu, în temeiul Normelor privind protecția datelor, aderarea la mecanismele de certificare aprobate poate servi drept dovadă a respectării obligațiilor prevăzute de Normele privind protecția datelor ([210]). În plus, în anumite condiții, Normele privind protecția datelor prevăd efectuarea unei evaluări a impactului asupra protecției datelor sau o consultare prealabilă a responsabilului cu protecția datelor și a Comitetului pentru protecția datelor. Este necesară o evaluare a impactului asupra protecției datelor în cazul în care un tip de prelucrare poate să genereze un risc ridicat pentru drepturile și libertățile unei persoane fizice ([211]). Acest lucru este necesar, de exemplu, în cazul în care există o evaluare sistematică și cuprinzătoare a aspectelor personale pe care se bazează deciziile automatizate sau în cazul în care se prelucrează categorii speciale de date la scară largă ([212]). În cazul în care o evaluare a impactului indică faptul că prelucrarea ar genera un risc ridicat pentru drepturile și libertățile persoanelor fizice, iar riscul nu poate fi atenuat prin măsuri de securitate rezonabile, operatorul trebuie să consulte Comitetul pentru protecția datelor ([213]). Comitetul pentru protecția datelor trebuie să ofere consiliere în scris în cazul în care consideră că prelucrarea preconizată ar încălca Normele privind protecția datelor ([214]). La un nivel mai general, operatorul are obligația de a consulta responsabilul cu protecția datelor atunci când pregătește norme sau documente operaționale cu privire la punerea în aplicare a restricțiilor privind drepturile individuale ([215]).

2.5. **Supravegherea și asigurarea respectării normelor**

(78) Pentru a asigura în practică un nivel adecvat de protecție a datelor, ar trebui instituită o autoritate de supraveghere independentă, care să aibă competența de a monitoriza și de a asigura respectarea normelor privind protecția datelor. Autoritatea respectivă ar trebui să acționeze cu deplină independență și imparțialitate în îndeplinirea sarcinilor sale și în exercitarea competențelor sale.

(79) Cadrul juridic al Organizației Europene de Brevete încredințează unui număr de două organisme supravegherea respectării normelor privind protecția datelor de către Organizația Europeană de Brevete: responsabilul cu protecția datelor și Comitetul pentru protecția datelor. Ambele organisme sunt create în temeiul articolului 32A din Statutul personalului, iar statutul și competențele lor sunt specificate mai în detaliu în Normele privind protecția datelor ([216]). Rolurile lor sunt complementare și implică cooperare, însă fiecare organism rămâne independent în ceea ce privește funcțiile sale respective.

([205]) Articolul 26 alineatul (1) din Normele privind protecția datelor.
([206]) Articolul 27 alineatele (1) și (2) din Normele privind protecția datelor.
([207]) Articolul 32 alineatele (1) și (2) din Normele privind protecția datelor. În temeiul articolului 4 alineatul (1) din Normele privind protecția datelor, operatorul trebuie să urmeze „o abordare structurată și bazată pe riscuri în ceea ce privește conceperea și documentarea operațiunilor de prelucrare". Operatorul trebuie, de asemenea, să fie în măsură să demonstreze în orice moment persoanelor vizate că angajamentele și condițiile documentate sunt respectate la efectuarea operațiunilor de prelucrare.
([208]) Articolul 32 alineatele (4), (5) și (6) din Normele privind protecția datelor.
([209]) Articolul 45 din Normele privind protecția datelor.
([210]) Articolul 26 alineatul (3) din Normele privind protecția datelor.
([211]) Operatorul trebuie să solicite consiliere din partea responsabilului cu protecția datelor cu privire la necesitatea de a efectua o evaluare a impactului, care, la rândul său, poate consulta Comitetul pentru protecția datelor în cazul în care există dubii în această privință. A se vedea articolul 38 alineatele (1)-(2) din Normele privind protecția datelor.
([212]) Articolul 38 alineatul (4) din Normele privind protecția datelor.
([213]) Articolul 38 alineatul (6) din Normele privind protecția datelor.
([214]) Articolul 38 alineatele (7) și (8) și articolul 39 din Normele privind protecția datelor.
([215]) Articolul 40 alineatul (2) din Normele privind protecția datelor.
([216]) Articolul 32A alineatele (1)-(2) din Statutul personalului, care prevede că responsabilul cu protecția datelor are rolul de a monitoriza aplicarea dispozițiilor privind protecția datelor cu caracter personal, de a consilia diferitele unități operaționale ale Organizației Europene de Brevete cu privire la îndeplinirea obligațiilor care le revin și de a le furniza documentația operațională necesară pentru punerea în aplicare practică a cerințelor privind protecția datelor. Comitetul pentru protecția datelor este obligat să asigure „o supraveghere independentă, eficace și imparțială a dispozițiilor aplicabile protecției datelor cu caracter personal". Poate exista un alt mecanism independent de supraveghere a respectării normelor de către camerele de recurs atunci când prelucrează date cu caracter personal în exercițiul funcției lor judiciare [a se vedea, de asemenea, articolul 2 alineatul (6) din Normele privind protecția datelor].

2.5.1. ***Independență***

(80) În temeiul Statutul personalului, responsabilul cu protecția datelor și Comitetul pentru protecția datelor acționează complet independent de orice interferență internă sau externă în îndeplinirea atribuțiilor care le revin și în exercitarea competențelor lor ([217]). Acest principiu este completat de diferite garanții suplimentare care le consacră independența.

(81) Responsabilul cu protecția datelor (și adjuncții săi) sunt numiți de președinte pe baza calificărilor lor profesionale și, în special, a cunoștințelor lor de specialitate în ceea ce privește legislația și practicile în materie de protecție a datelor ([218]). Responsabilul cu protecția datelor este numit pentru un mandat de trei până la cinci ani, care poate fi reînnoit. Comitetul pentru protecția datelor este consultat înainte de orice propunere de revocare sau de eliberare din funcție a responsabilului cu protecția datelor ([219]). O astfel de consultare prealabilă înainte de revocarea sau eliberarea din funcție a responsabilului cu protecția datelor este menită să asigure un control și o analiză suplimentare în cazul unei propuneri de revocare sau de eliberare din funcție. O astfel de revocare sau eliberare din funcție poate fi propusă din unul dintre următoarele motive ([220]): în cazul în care responsabilul cu protecția datelor nu mai îndeplinește condițiile necesare pentru îndeplinirea atribuțiilor ([221]), pentru incompetență profesională ([222]) sau ca urmare a unor măsuri disciplinare ([223]). Normele privind protecția datelor stabilesc, de asemenea, că responsabilul cu protecția datelor nu poate fi eliberat din funcție sau sancționat pentru îndeplinirea atribuțiilor sale și nu poate primi instrucțiuni ([224]). Responsabilul cu protecția datelor trebuie să fie implicat în toate aspectele legate de protecția datelor cu caracter personal și elaborează rapoarte anuale de activitate adresate președintelui și Consiliului de administrație ([225]). Oficiul trebuie să pună la dispoziția responsabilului cu protecția datelor resursele necesare pentru îndeplinirea atribuțiile sale ([226]).

(82) Comitetul pentru protecția datelor este format din trei experți externi în domeniul protecției datelor, și anume un președinte și alți doi membri ([227]), precum și un membru supleant, numit de președintele Organizației Europene de Brevete pentru un mandat de trei ani, care poate fi reînnoit ([228]). Membrii Comitetului pentru protecția datelor trebuie să dețină calificările necesare pentru numirea în funcții judiciare sau să fie profesioniști în domeniul protecției datelor cu cunoștințe de specialitate și experiență dovedite în domeniul legislației privind protecția datelor, dobândite la nivel național sau internațional. Aceștia nu trebuie să fie angajați ai Organizației Europene de Brevete sau să fi fost angajați de aceasta în ultimii zece ani ([229]). În temeiul articolului 48 alineatul (6) din Normele privind protecția datelor, membrii Comitetului pentru protecția datelor trebuie să fie complet independenți în exercitarea funcției lor. În special, membrii Comitetului pentru protecția datelor nu pot solicita instrucțiuni de la Oficiu sau de la Consiliul de administrație și nu pot fi obligați să respecte astfel de instrucțiuni. Regulamentul de procedură al Comitetului pentru protecția datelor prevede de asemenea că acesta trebuie să acționeze în mod imparțial și în deplină independență în îndeplinirea atribuțiilor sale ([230]). În plus, membrii Comitetului pentru protecția datelor pot

([217]) Articolul 32A alineatele (4) și (5) din Statutul personalului.

([218]) Articolul 41 din Normele privind protecția datelor.

([219]) Articolul 42 alineatul (8) din Normele privind protecția datelor. Această consultare are loc indiferent de motivul oricărei propuneri de revocare sau de concediere.

([220]) Articolul 50 din Statutul personalului.

([221]) A se vedea articolul 53 alineatul (1) din Statutul personalului, care prevede că „[a]utoritatea împuternicită să facă numiri poate decide încetarea raporturilor de muncă ale unui angajat: (a) dacă statul contractant al cărui resortisant este angajatul încetează să mai fie parte la convenție, (b) în cazul în care angajatul refuză să fie transferat într-o altă țară decât cea în care își desfășoară activitatea, (c) dacă, în cazul unui angajat numit de Consiliul de administrație în conformitate cu articolul 11 alineatele (1) și (2) din Convenție, Consiliul de administrație decide astfel în interesul organizației, (d) în cazul unui angajat care a desfășurat o activitate neîntreruptă de cel mult un an în cadrul unei numiri pe durată determinată, (e) în cazul în care, în urma propriilor acțiuni, acesta nu mai îndeplinește condițiile prevăzute la articolul 8 litera (a) sau (b) [și anume de a fi resortisant al unuia dintre statele contractante ale Organizației Europene de Brevete, cu excepția cazului în care autoritatea împuternicită să facă numiri autorizează o excepție în acest sens, precum și de a beneficia de drepturi cetățenești depline] sau (f) în celelalte cazuri prevăzute în mod expres în prezentul Statut al personalului".
A se vedea de asemenea articolul 13 alineatul (4) litera (b) din Statutul personalului, care prevede că „un raport privind persoana aflată în perioada de probă poate fi întocmit în orice moment al perioadei de probă, în cazul în care îndeplinirea atribuțiilor, eficiența și conduita acesteia se dovedesc a fi inadecvate. Pe baza raportului sau rapoartelor privind perioada de probă, autoritatea împuternicită să facă numiri poate:
— elibera din funcție un angajat nou-recrutat aflat în perioada de probă;
— decide ca persoana aflată în perioada de probă care a fost transferată, promovată sau repartizată într-un alt post să revină fie pe postul anterior, fie, în cazul în care acesta a fost ocupat, pe un post corespunzător gradului postului său anterior pentru care îndeplinește cerințele".

([222]) Articolul 52 din Statutul personalului prevede criteriile și procesele care trebuie urmate în cazul unei „incompetențe profesionale" identificate.

([223]) Articolul 94 din Statutul personalului.

([224]) Articolul 42 alineatul (3) din Normele privind protecția datelor. Deși responsabilul cu protecția datelor poate îndeplini și alte atribuții, aceste atribuții nu trebuie să conducă la un conflict de interese [articolul 42 alineatul (6) din Normele privind protecția datelor].

([225]) Articolul 42 alineatele (1) și (3) din Normele privind protecția datelor.

([226]) Articolul 42 alineatul (2) din Normele privind protecția datelor.

([227]) Articolul 48 alineatul (1) din Normele privind protecția datelor.

([228]) Articolul 48 alineatele (1) și (3) din Normele privind protecția datelor.

([229]) Articolul 48 alineatul (2) din Normele privind protecția datelor.

([230]) Articolul 1 alineatul (1) din Regulamentul de procedură al Comitetului pentru protecția datelor, CA/26/21 Add. 1, adoptat la 11 iunie 2021. Acesta este disponibil la adresa https://link.epo.org/web/data_protection_board-rules_of_procedure_en.pdf.

fi eliberați din funcție de Organizația Europeană de Brevete numai în baza unor motive grave ([231]). Membrii Comitetului pentru protecția datelor sunt supuși unei obligații de confidențialitate ([232]) și nu trebuie să acționeze într-un caz în care există un conflict de interese, în special un interes personal ([233]). Organizația Europeană de Brevete trebuie să sprijine Comitetul pentru protecția datelor în îndeplinirea atribuțiilor sale, oferindu-i resursele necesare, precum și sprijin juridic și administrativ (prin intermediul unui secretariat și oferind Comitetului pentru protecția datelor acces la datele cu caracter personal și la operațiunile de prelucrare) ([234]).

2.5.2. ***Atribuții și competențe***

(83) Printre atribuțiile responsabilului cu protecția datelor se numără următoarele: informarea operatorului sau a persoanelor împuternicite de operator cu privire la obligațiile care le revin și consilierea acestora în consecință, sensibilizarea și formarea personalului implicat în operațiunile de prelucrare, asigurarea faptului că persoanele vizate sunt informate în privința drepturilor lor în temeiul Normelor privind protecția datelor și monitorizarea în mod independent a aplicării interne și a respectării Normelor privind protecția datelor, precum și a altor dispoziții legale ale Organizației Europene de Brevete care au implicații în materie de protecție a datelor ([235]). Persoanele vizate pot contacta responsabilul cu protecția datelor cu privire la orice aspect legat de prelucrarea datelor lor sau de exercitarea drepturilor lor ([236]), iar operatorul și persoanele împuternicite de operator pot consulta responsabilul cu protecția datelor cu privire la orice aspect referitor la interpretarea și aplicarea Normelor privind protecția datelor ([237]).

(84) În cadrul rolului său de supraveghere, responsabilul cu protecția datelor are competența de a efectua audituri și investigații privind protecția datelor ([238]). Auditurile sunt inițiate de responsabilul cu protecția datelor în conformitate cu un plan anual de audit care este elaborat în consultare cu Comitetul pentru protecția datelor ([239]). Auditurile se axează pe evaluarea evidențelor, a declarațiilor și a documentației relevante în materie de protecție a datelor, de exemplu pentru a verifica exactitatea și exhaustivitatea documentației relevante în materie de protecție a datelor, aplicarea corectă a metodologiilor de gestionare a riscurilor, acuratețea și promptitudinea răspunsurilor adresate persoanelor vizate sau buna desfășurare a evaluărilor impactului asupra protecției datelor și numărul acestora ([240]). Potrivit informațiilor primite de Comisie de la responsabilul cu protecția datelor, s-au efectuat trei audituri în 2023, respectiv patru în 2024. O investigație poate fi inițiată de responsabilul cu protecția datelor din proprie inițiativă, pe baza unei cereri primite de la Comitetul pentru protecția datelor sau de la un organism din cadrul Organizației Europene de Brevete (de exemplu, președintele sau un operator delegat) sau pe baza informațiilor primite în alt mod (inclusiv, de exemplu, de la părți terțe și persoane fizice) ([241]). Investigațiile solicitate de Comitetul pentru protecția datelor sunt efectuate de responsabilul cu protecția datelor în mod independent. Comitetul pentru protecția datelor poate prezenta observații și/sau poate solicita o investigație suplimentară cu privire la orice problemă care ar putea apărea ([242]). Controalele se axează pe operațiunile de prelucrare sau pe aspecte specifice ale acestora ori pe evenimente legate de acestea, urmărind asigurarea faptului că prelucrarea în cauză îndeplinește cerințele Normelor privind protecția datelor, precum și asigurarea protecției drepturilor și libertăților persoanelor vizate ([243]).

(85) Responsabilul cu protecția datelor are acces la toate informațiile relevante, inclusiv la datele cu caracter personal prelucrate, precum și la toate serviciile, instalațiile de prelucrare a datelor și suporturile de date ([244]). Toți angajații Organizației Europene de Brevete și unitățile operaționale trebuie să asiste responsabilul cu protecția datelor în îndeplinirea atribuțiilor sale, inclusiv prin asigurarea accesului în spațiile fizice și la informații relevante ([245]).

([231]) În special, contractul prevede că acesta „poate fi reziliat [numai], fără a aduce atingere dreptului de reziliere din motive grave, de către [membrul Comitetului pentru protecția datelor] cu un preaviz scris de șase (6) luni". Întrucât contractul de prestări de servicii este reglementat de dreptul german, noțiunea de motiv grav trebuie interpretată în conformitate cu articolul 626 din Codul civil german. Potrivit jurisprudenței, această situație poate interveni, de exemplu, în cazul încălcării repetate și persistente a obligațiilor aplicabile (de exemplu, în ceea ce privește conflictul de interese) sau în cazul detenției.

([232]) Articolul 48 alineatul (5) din Normele privind protecția datelor.

([233]) Articolul 48 alineatul (7) din Normele privind protecția datelor.

([234]) Articolul 48 alineatul (10) din Normele privind protecția datelor. Secretariatul își îndeplinește atribuțiile independent de orice interferență nejustificată și exclusiv în conformitate cu instrucțiunile președintelui Comitetului pentru protecția datelor. Acesta oferă sprijin juridic, administrativ și logistic comitetului. A se vedea articolul 2 din Regulamentul de procedură al Comitetului pentru protecția datelor.

([235]) Articolul 43 alineatul (1) din Normele privind protecția datelor.

([236]) Articolul 43 alineatul (1) litera (k) din Normele privind protecția datelor.

([237]) Articolul 42 alineatele (4) și (7) din Normele privind protecția datelor.

([238]) Articolul 43 alineatul (1) litera (d) din Normele privind protecția datelor. A se vedea, de asemenea, nota privind supravegherea protecției datelor intitulată „*How the Data Protection Office Conducts DP Audits and DP Inspections*" (Desfășurarea auditurilor și a controalelor cu privire la protecția datelor de către serviciul responsabil cu protecția datelor), disponibilă la adresa https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-data-protection-oversight-mechanism.pdf.

([239]) Comitetul pentru protecția datelor poate formula sugestii cu privire la domeniile în care ar trebui efectuate audituri; a se vedea Nota privind supravegherea protecției datelor, p. 4.

([240]) Nota privind supravegherea protecției datelor, p. 4.

([241]) Nota privind supravegherea protecției datelor, p. 7.

([242]) Nota privind supravegherea protecției datelor, p. 6.

([243]) Nota privind supravegherea protecției datelor, p. 6.

([244]) Articolul 43 alineatul (5) din Normele privind protecția datelor.

([245]) Articolul 46 din Normele privind protecția datelor.

(86) Atunci când încheie un audit sau o investigație, responsabilul cu protecția datelor adoptă un raport, în care prezintă constatările, concluziile și măsurile de remediere recomandate ([246]). Astfel de măsuri pot include, de exemplu, măsuri preventive sau de atenuare pentru îmbunătățirea conformității, precum și măsuri de remediere a neconformității (de exemplu alinierea prelucrării la Normele privind protecția datelor, gestionarea cererilor de exercitare a drepturilor înaintate de persoanele vizate, suspendarea sau încetarea unei prelucrări etc.) ([247]). Responsabilul cu protecția datelor poate, de asemenea, să aducă în atenția autorității competente împuternicite să facă numiri cazurile de nerespectare a Normelor privind protecția datelor de către angajați și să recomande inițierea unei anchete administrative pentru a stabili dacă sunt necesare măsuri disciplinare sau de altă natură ([248]). Orice angajat care nu respectă Normele privind protecția datelor, în mod intenționat sau din neglijență, poate fi pasibil de sancțiuni disciplinare sau de alte măsuri în temeiul Statutului personalului ([249]).

(87) Rezultatele auditurilor și ale investigațiilor trebuie comunicate Comitetului pentru protecția datelor ([250]). Raportul de audit sau raportul elaborat în urma investigației trebuie comunicat, la cerere, Comitetului pentru protecția datelor. Comitetul pentru protecția datelor este autorizat să prezinte observații cu privire la raportul responsabilului cu protecția datelor, inclusiv cu privire la constatările responsabilului cu protecția datelor referitoare la existența sau inexistența unei încălcări a Normelor privind protecția datelor sau cu privire la măsurile de remediere propuse, și poate solicita măsuri de investigare suplimentare ([251]). În cazul în care, în urma unui audit sau a unui control efectuat de responsabilul cu protecția datelor, se concluzionează că a existat o neconformitate (și anume o încălcare a Normelor privind protecția datelor), raportul responsabilului cu protecția datelor trebuie prezentat Comitetului pentru protecția datelor pentru validarea concluziilor și a măsurilor de remediere recomandate. În cazul în care Comitetul pentru protecția datelor nu este de acord cu concluziile sau cu măsurile de remediere recomandate de responsabilul cu protecția datelor, Comitetul pentru protecția datelor transmite observațiile sale responsabilului cu protecția datelor, inclusiv în vederea modificării concluziilor propuse și a măsurilor de remediere recomandate, iar acesta ar trebui să le pună în aplicare în consecință. Măsurile de remediere validate de Comitetul pentru protecția datelor sunt obligatorii pentru operator și pentru operatorii delegați și pot fi invocate de persoanele fizice înaintea mecanismele de recurs descrise în considerentul 95 ([252]). Responsabilul cu protecția datelor trebuie să verifice punerea în aplicare a măsurilor de remediere (în principiu după șase luni de la comunicarea acestora) și să raporteze anual președintelui cu privire la stadiul punerii în aplicare ([253]).

(88) Pe lângă rolul său de a asigura respectarea Normelor privind protecția datelor, alte sarcini ale Comitetului pentru protecția datelor includ consilierea președintelui cu privire la adoptarea deciziilor privind caracterul adecvat al nivelului de protecție, consilierea operatorului cu privire la necesitatea de a efectua o evaluare a impactului asupra protecției datelor și examinarea plângerilor din partea persoanelor fizice (a se vedea considerentele 92-96) ([254]).

2.6. **Reparații**

(89) Pentru asigurarea unei protecții adecvate și, în special, pentru asigurarea respectării drepturilor individuale, persoanei vizate ar trebui să i se ofere reparații efective, inclusiv despăgubiri pentru prejudiciile suferite.

(90) Cadrul juridic al Organizației Europene de Brevete oferă reparații persoanelor fizice printr-o combinație de căi de atac diferite.

(91) În primul rând, persoanele vizate care consideră că prelucrarea datelor lor cu caracter personal de către Organizația Europeană de Brevete le încalcă drepturile (și anume încalcă Normele privind protecția datelor) pot depune o cerere de reexaminare de către operatorul delegat în conformitate cu articolul 49 din Normele privind protecția datelor. Operatorul delegat va examina plângerea și va lua o decizie ([255]). Înainte de a lua o decizie, operatorul delegat trebuie să consulte responsabilul cu protecția datelor, care emite un aviz scris în termen de cel mult cincisprezece zile calendaristice de la primirea cererii de reexaminare ([256]). Operatorul delegat trebuie să răspundă persoanei fizice în

([246]) Nota privind supravegherea protecției datelor.
([247]) Nota privind supravegherea protecției datelor, p. 2 (definiția „recomandărilor").
([248]) Articolul 43 alineatul (6) din Normele privind protecția datelor.
([249]) Articolul 54 din Normele privind protecția datelor. Sancțiunile disciplinare sunt impuse de președinte, care exercită autoritate disciplinară și are competențe disciplinare în ceea ce privește personalul Organizației Europene de Brevete – a se vedea articolul 10 din CBE și articolul 93 și următoarele din Statutul personalului.
([250]) Nota privind supravegherea protecției datelor, p. 7.
([251]) Nota privind supravegherea protecției datelor, p. 3 și p. 8.
([252]) Decizia președintelui Oficiului European de Brevete din 12.7.2024 privind forța executorie a recomandărilor responsabilului cu protecția datelor aprobate de Comitetul pentru protecția datelor în cadrul auditurilor și controalelor privind protecția datelor, https://link.epo.org/web/office/data-protection-and-privacy/en-decision-of-the-president-on-enforceability-of-dpo-conclusions-and-recommendations.pdf.
([253]) Nota privind supravegherea protecției datelor, p. 5 și p. 9.
([254]) Articolul 47 din Normele privind protecția datelor.
([255]) Articolul 49 alineatul (1) din Normele privind protecția datelor. Cererea trebuie înaintată în termen de cel mult trei luni de la data la care persoana vizată a fost informată sau a luat cunoștință în alt mod de prelucrarea datelor cu caracter personal despre care se presupune că îi încalcă drepturile.
([256]) Articolul 49 alineatul (2) din Normele privind protecția datelor. În cazul în care responsabilul cu protecția datelor nu emite un aviz până la sfârșitul acestei perioade, avizul respectiv nu mai este necesar.

cauză în termen de o lună de la data primirii cererii ([257]). Decizia trebuie comunicată persoanei fizice în cauză, împreună cu informații privind posibilitatea de a obține reparații suplimentare ([258]). În cazul în care operatorul delegat nu ia nicio măsură în termen de trei luni, acest lucru este considerat o respingere implicită a cererii.

(92) În al doilea rând, persoanele fizice pot contesta o decizie sau o respingere implicită a unei cereri de reexaminare de către un operator delegat prin depunerea unei plângeri la Comitetul pentru protecția datelor ([259]).

(93) Atunci când examinează o plângere, Comitetul pentru protecția datelor trebuie să invite persoana vizată, operatorul și, după caz, persoana împuternicită de operator să își prezinte în scris poziția cu privire la afirmațiile și faptele în cauză și să furnizeze dovezi sau observații și argumente cu privire la dovezile disponibile ([260]). În acest context, Comitetul pentru protecția datelor poate solicita părților orice informație necesară pentru gestionarea plângerii și, în plus, poate obține informații suplimentare prin intermediul responsabilului cu protecția datelor ([261]). Atunci când decide cu privire la măsurile care trebuie luate în urma unei plângeri, Comitetul pentru protecția datelor trebuie să țină seama, printre altele, de natura și gravitatea presupusei încălcări, de numărul de persoane vizate afectate, de categoriile de date afectate și de durata încălcării ([262]). Comitetul pentru protecția datelor poate invita părțile să soluționeze diferendul pe cale amiabilă și încurajează și facilitează în mod activ o astfel de soluționare ([263]). De asemenea, reclamantul poate solicita Comitetului pentru protecția datelor să aplice o procedură de urgență, din motive de gravitate a presupusei încălcări sau ca urmare a gravității riscului asupra drepturilor persoanelor fizice ([264]).

(94) După examinarea unei plângeri, Comitetul pentru protecția datelor emite un aviz motivat adresat operatorului, care include o expunere a faptelor, principalele argumente ale părților, precum și considerațiile și recomandările Comitetului pentru protecția datelor ([265]). În cazul unei proceduri de urgență, Comitetul pentru protecția datelor trebuie să emită în mod oficial un aviz motivat în termen de două luni de la depunerea plângerii ([266]). În avizul său motivat, Comitetul pentru protecția datelor poate emite orice recomandări pe care le consideră necesare, inclusiv măsuri de încetare (de exemplu încetarea prelucrării ilegale a datelor sau ștergerea datelor prelucrate în mod ilegal) și despăgubiri pentru prejudicii materiale sau morale ([267]). Avizul motivat trebuie comunicat persoanei vizate și operatorului (și anume președintelui Oficiului, președintelui camerelor de recurs, președintele consiliului de administrație sau președintele comitetului restrâns, în funcție de destinatarul plângerii: Oficiul, camerele de recurs, Consiliul sau comitetul restrâns). Operatorul va lua apoi o decizie finală obligatorie, în urma avizului motivat al Comitetului pentru protecția datelor ([268]). Decizia finală este comunicată persoanei vizate, Comitetului pentru protecția datelor și responsabilului cu protecția datelor ([269]). În cazul în care operatorul decide să nu țină seama de unul sau mai multe aspecte ale avizului motivat, acesta îl explică în scris în decizie ([270]).

(95) O persoană vizată care nu este mulțumită de decizia operatorului poate recurge la o altă cale de atac și poate face trimitere la avizul motivat al Comitetului pentru protecția datelor. Angajații Organizației Europene de Brevete pot contesta decizia înaintea Tribunalului Administrativ al Organizației Internaționale a Muncii ([271]). Orice altă persoană vizată care nu este de acord cu decizia operatorului poate să prezinte președintelui o cerere de arbitraj ad-hoc în termen de trei luni de la primirea deciziei ([272]). Normele privind protecția datelor prevăd o procedură specifică ce trebuie urmată în cazul

([257]) Articolul 49 alineatul (3) din Normele privind protecția datelor. Acest termen poate fi prelungit cu încă două luni atunci când este necesar, ținându-se seama de complexitatea și de numărul cererilor. În cazul prelungirii, operatorul delegat trebuie să notifice persoanei vizate acest lucru și motivele întârzierii în termen de o lună de la primirea cererii de reexaminare.

([258]) Articolul 49 alineatul (3) din Normele privind protecția datelor.

([259]) Articolul 50 alineatul (1) din Normele privind protecția datelor. O plângere înaintea Comitetului pentru protecția datelor trebuie formulată în termen de trei luni de la primirea deciziei sau, în cazul unei respingeri implicite, de la data expirării termenului de răspuns la cerere.

([260]) Articolul 50 alineatul (2) din Normele privind protecția datelor.

([261]) În special, responsabilul cu protecția datelor are obligația de a răspunde cererilor adresate de Comitetul pentru protecția datelor și de a coopera cu acesta [articolul 43 litera (i) din Normele privind protecția datelor]. Responsabilul cu protecția datelor are, de asemenea, obligația de a facilita cooperarea dintre Comitetul pentru protecția datelor și Oficiu și, în acest context, are acces la orice informații relevante [articolul 43 litera (j), articolul 46 literele (a) și (b) din Normele privind protecția datelor].

([262]) Articolul 4 alineatul (5) din Regulamentul de procedură al Comitetului pentru protecția datelor.

([263]) Articolul 8 din Regulamentul de procedură al Comitetului pentru protecția datelor.

([264]) Articolul 11 alineatul (1) din Regulamentul de procedură al Comitetului pentru protecția datelor.

([265]) Articolul 10 alineatul (2) din Regulamentul de procedură al Comitetului pentru protecția datelor.

([266]) Articolul 11 alineatul (2) din Regulamentul de procedură al Comitetului pentru protecția datelor.

([267]) Articolul 50 alineatul (3) din Normele privind protecția datelor.

([268]) Articolul 50 alineatul (4) din Normele privind protecția datelor și articolul 10 alineatul (6) din Regulamentul de procedură al Comitetului pentru protecția datelor.

([269]) Articolul 50 alineatul (6) din Normele privind protecția datelor.

([270]) Articolul 50 alineatul (4) din Normele privind protecția datelor. În cazul în care recomandările Comitetului pentru protecția datelor nu sunt direct relevante pentru persoanele vizate, orice abatere se stabilește în scris de către operator prin intermediul unui document transmis DPB.

([271]) Articolul 50 alineatul (7) din Normele privind protecția datelor. A se vedea articolul 13 din CBE și articolul 113 din Statutul personalului.

([272]) Articolul 50 alineatul (8) și articolul 52 alineatul (2) din Normele privind protecția datelor. În temeiul Normelor privind protecția datelor ale Consiliului de administrație și al Normelor privind protecția datelor ale Comitetului restrâns, se poate solicita arbitrajul din partea președintelui Consiliului de administrație.

arbitrajului ad-hoc ([273]). În special, în termen de trei luni de la primirea cererii de către persoana vizată, secretarul general al Curții Permanente de Arbitraj trebuie să numească un arbitru pe baza criteriilor stabilite în Normele privind protecția datelor ([274]). Arbitrul trebuie să fie calificat din punct de vedere juridic, să fie autorizat să practice dreptul într-unul dintre statele contractante ale Organizației Europene de Brevete, să poată demonstra cunoștințe de specialitate relevante în materie de protecție a datelor și să fie familiarizat cu legislația care reglementează organizațiile internaționale ([275]). Pe lângă îndeplinirea acestor criterii, pot fi desemnate numai persoanele care nu au desfășurat activități în calitate de angajați ai Organizației Europene de Brevete sau ai persoanei vizate sau în serviciul acestora. Normele privind protecția datelor prevăd că arbitrul trebuie să acționeze independent și imparțial ([276]), să trateze fiecare parte în mod egal și să le ofere posibilitatea de a-și prezenta cauza în fiecare etapă a procedurilor ([277]). Procedurile de arbitraj nu sunt publice ([278]) și sunt reglementate de CBE, Normele privind protecția datelor, inclusiv de orice legislație de punere în aplicare, dreptul organizațiilor internaționale și principiile dreptului internațional public ([279]). Deși fiecare parte are obligația de a-și suporta propriile cheltuieli și costuri de reprezentare juridică (cu excepția cazului în care arbitrul decide altfel), onorariile și cheltuielile arbitrului, precum și costurile aferente eventualelor consilieri de specialitate și martorilor sunt suportate de Organizația Europeană de Brevete ([280]). Tranzacțiile se încheie sub forma unei hotărâri arbitrale scrise, cu o formulare convenită, care este definitivă și obligatorie ([281]).

(96) Orice persoană care a suferit prejudicii ca urmare a unei încălcări a Normelor privind protecția datelor poate solicita despăgubiri Organizației Europene de Brevete utilizând procedurile descrise în considerentele 91-95 ([282]). Organizația Europeană de Brevete nu va fi considerată răspunzătoare dacă se dovedește că nu a fost responsabilă pentru evenimentul care a cauzat prejudiciul.

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

(97) Cadrul juridic în temeiul căruia Organizația Europeană de Brevete analizează cererile din partea autorităților publice – din statele sale contractante și din țările terțe – și răspunde cererilor acestora cu privire la datele cu caracter personal prelucrate de Organizația Europeană de Brevete decurge din Protocolul Organizației Europene de Brevete cu privire la privilegii și imunități ([283]), din cerințele Normelor privind protecția datelor referitoare la transmiterea și transferurile de date cu caracter personal și din dreptul internațional public.

(98) În primul rând, prelucrarea datelor cu caracter personal de către Organizația Europeană de Brevete în scopul activităților sale oficiale este acoperită de imunitățile conferite organizației. Imunitățile Organizației Europene de Brevete sunt completate de o obligație de cooperare prevăzută la articolul 20 din Protocolul cu privire la privilegii și imunități. În consecință, orice cerere din partea unei autorități publice a unui stat contractant de a obține date prelucrate de Organizația Europeană de Brevete trebuie analizată de președinte în conformitate cu [articolul 20 alineatul (1)] din Protocolul cu privire la privilegii și imunități, care prevede că organizația „cooperează în orice moment cu autoritățile competente ale statelor contractante pentru a facilita buna administrare a justiției, pentru a asigura respectarea reglementărilor polițienești și a reglementărilor privind sănătatea publică, inspecția muncii sau alte legislații naționale similare și pentru a preveni orice abuz de privilegii, imunități și facilități prevăzute de prezentul protocol." Cu titlu excepțional, organizația poate renunța la imunitatea de jurisdicție și de executare ([284]). Atunci când decide cu privire la o cerere de cooperare, președintele își exercită puterea discreționară, având în vedere conformitatea cererii cu cadrul juridic al organizației ([285]). Se poate concluziona că Oficiul poate răspunde unei cereri în temeiul Protocolului cu privire la privilegii și imunități și poate divulga date cu caracter personal numai în conformitate cu cerințele privind transmiterea de date prevăzute în Normele privind protecția datelor (a se vedea considerentele 62-67). În conformitate cu Normele privind protecția datelor, destinatarul trebuie să furnizeze 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 (statele contractante) în cauză ([286]). Operatorul trebuie să fie în măsură,

([273]) Articolul 52 alineatul (1) din Normele privind protecția datelor.
([274]) Articolul 52 alineatul (4) din Normele privind protecția datelor.
([275]) Articolul 52 alineatul (4) din Normele privind protecția datelor.
([276]) Articolul 52 alineatul (4) din Normele privind protecția datelor.
([277]) Articolul 52 alineatul (8) din Normele privind protecția datelor.
([278]) Articolul 52 alineatul (9) din Normele privind protecția datelor.
([279]) Articolul 52 alineatul (6) din Normele privind protecția datelor. Locul de desfășurare al arbitrajului este Haga [articolul 52 alineatul (5) din Normele privind protecția datelor], iar limba utilizată în cursul procedurii trebuie aleasă de arbitru, aceasta trebuind totuși să fie una dintre limbile oficiale ale Organizației Europene de Brevete (engleză, franceză sau germană) [articolul 52 alineatul (7) din Normele privind protecția datelor].
([280]) Articolul 52 alineatul (13) din Normele privind protecția datelor.
([281]) Articolul 52 alineatul (10) din Normele privind protecția datelor. A se vedea, de asemenea, articolul 3 și articolul 34 alineatul (2) din Regulamentul Curții Permanente de Arbitraj.
([282]) Articolul 53 din Normele privind protecția datelor. În anumite condiții (în special ținând seama de cerințele aplicabile în temeiul legislației germane), persoanele fizice pot obține, de asemenea, despăgubiri pentru prejudiciile cauzate de personalul Organizației Europene de Brevete în exercitarea atribuțiilor lor, în temeiul articolului 9 alineatul (2) din CBE.
([283]) Protocolul Organizației Europene de Brevete cu privire la privilegii și imunități. Acesta este disponibil la adresa https://www.epo.org/en/legal/epc/2020/proprim.html.
([284]) Articolul 3 alineatul (1) litera (a) din Protocolul cu privire la privilegii și imunități.
([285]) Aceasta include posibilitatea de a respinge o cerere.
([286]) Articolul 8 alineatul (3) din Normele privind protecția datelor.

pentru fiecare transmitere de date, să demonstreze că o astfel de transmitere este necesară și proporțională cu scopul specific pentru care este realizată ([287]). Orice transmitere de date trebuie efectuată într-un mod care să asigure menținerea nivelului de protecție oferit de Normele privind protecția datelor ([288]). Potrivit orientărilor emise de responsabilul cu protecția datelor, aceasta înseamnă că sunt instituite garanții adecvate, inclusiv prin asigurarea faptului că datele care urmează să fie partajate trebuie reduse la minimum și limitate la ceea ce este adecvat, relevant și strict necesar pentru atingerea scopului respectiv ([289]). În cazul în care există orice motiv să se presupună că drepturile și libertățile persoanei în cauză pot fi afectate, operatorul trebuie să stabilească faptul că transmiterea datelor cu caracter personal în acest scop specific este proporțională, după punerea în balanță a diferitelor interese aflate în joc ([290]).

(99) În al doilea rând, nu există niciun instrument juridic aplicabil Organizației Europene de Brevete care să reglementeze în mod specific gestionarea cererilor autorităților publice din țări terțe (și anume care nu sunt părți contractante la Organizația Europeană de Brevete) de a obține date prelucrate de Organizația Europeană de Brevete. Prin urmare, orice divulgare ca răspuns la o astfel de cerere poate avea loc numai dacă sunt îndeplinite cerințele pentru transferurile internaționale de date în temeiul Normelor privind protecția datelor (astfel cum sunt descrise în considerentele 68-73). Acest lucru ar fi valabil numai dacă a fost adoptată o decizie privind caracterul adecvat al nivelului de protecție pentru țara relevantă care ar acoperi transferul, dacă există garanții adecvate sau dacă se aplică o derogare.

(100) Respectarea de către președinte a Protocolului cu privire la privilegii și imunități, inclusiv modul în care au fost abordate cererile de cooperare din partea autorităților publice, face obiectul supravegherii de către Consiliul de administrație, în timp ce respectarea cerințelor privind transmiterea și transferurile de date cu caracter personal din Normele privind protecția datelor face obiectul supravegherii de către responsabilul cu protecția datelor și Comitetul pentru protecția datelor, astfel cum se descrie în considerentele 84-88. Persoanele fizice pot utiliza căile de atac descrise în considerentele 90-96 în legătură cu transmiterea sau transferul datelor cu caracter personal ale acestora cu încălcarea Normelor privind protecția datelor.

4. CONCLUZII

(101) Comisia consideră că Organizația Europeană de Brevete asigură un nivel de protecție a datelor cu caracter personal transferate din Uniune în esență echivalent cu cel garantat de Regulamentul (UE) 2016/679.

(102) Pe baza constatărilor prezentei decizii, ar trebui să se decidă că Organizația Europeană de Brevete asigură un nivel de protecție adecvat în sensul articolului 45 din Regulamentul (UE) 2016/679, interpretat în lumina Cartei drepturilor fundamentale a Uniunii Europene, pentru datele cu caracter personal transferate din Uniune către Organizația Europeană de Brevete.

5. EFECTELE PREZENTEI DECIZII ȘI ACȚIUNILE AUTORITĂȚILOR PENTRU PROTECȚIA DATELOR

(103) Statele membre și organele acestora au obligația de a lua măsurile necesare pentru a se conforma actelor instituțiilor Uniunii, întrucât se presupune că aceste acte sunt legale și, prin urmare, produc efecte juridice atât timp cât nu sunt retrase, anulate în cadrul unei acțiuni în anulare sau declarate nule ca urmare a unei trimiteri preliminare sau a unei excepții de nelegalitate.

(104) În consecință, o decizie a Comisiei privind caracterul adecvat al nivelului de protecție, adoptată în temeiul articolului 45 alineatul (3) din Regulamentul (UE) 2016/679, este obligatorie pentru toate organele statelor membre cărora li se adresează, inclusiv pentru autoritățile de supraveghere independente ale acestora. În special, transferurile de la un operator sau o persoană împuternicită de operator din Uniune către Organizația Europeană de Brevete poate avea loc fără a fi necesară obținerea unei autorizări suplimentare.

([287]) Articolul 8 alineatul (4) din Normele privind protecția datelor.

([288]) Nota explicativă intitulată „*EPO transmission and transfer of personal data*” (Transmiterea și transferul de date la nivelul Organizației Europene de Brevete) (Nota de transmitere si transfer), disponibilă la adresa https://link.epo.org/web/office/data-protection-and-privacy/en-explanatory-note-on-epo-transmission-and-transfer-of-personal-data.pdf, nota de subsol 4. A se vedea, în special, „Normele privind protecția datelor ale Organizației Europene de Brevete […] stabilește principiul general al protecției adecvate, aplicabil în special fluxului internațional de date”.

([289]) Nota de subsol 12 din Nota de transmitere și transfer.

([290]) Articolul 8 alineatul (3) din Normele privind protecția datelor.

(105) Ar trebui reamintit faptul că, în temeiul articolului 58 alineatul (5) din Regulamentul (UE) 2016/679 și astfel cum este explicat de Curtea de Justiție în cauza C-362/14 ([291]), în cazul în care o autoritate națională pentru protecția datelor pune sub semnul întrebării, inclusiv în urma primirii unei plângeri, compatibilitatea unei decizii a Comisiei privind caracterul adecvat al nivelului de protecție cu dreptul fundamental al unei persoane la viață privată și la protecția datelor, legislația națională trebuie să prevadă o cale de atac pentru a invoca motivele respective în fața unei instanțe naționale, care poate fi obligată să efectueze o trimitere preliminară către Curtea de Justiție.

6. MONITORIZAREA, SUSPENDAREA, ABROGAREA SAU MODIFICAREA PREZENTEI DECIZII

(106) În conformitate cu jurisprudența Curții de Justiție și în temeiul articolului 45 alineatul (4) din Regulamentul (UE) 2016/679, Comisia ar trebui să monitorizeze continuu evoluțiile relevante din țara terță sau de la nivelul organizației internaționale după adoptarea unei decizii privind caracterul adecvat al nivelului de protecție, pentru a evalua dacă aceasta continuă să asigure un nivel de protecție în esență echivalent. O astfel de verificare se impune, în orice caz, atunci când Comisia primește orice informație care dă naștere unor îndoieli justificate în această privință.

(107) Prin urmare, Comisia ar trebui să monitorizeze în permanență situația de la nivelul Organizației Europene de Brevete în ceea ce privește cadrul juridic și practica propriu-zisă de prelucrare a datelor cu caracter personal, astfel cum sunt evaluate în prezenta decizie. Pentru a facilita acest proces, Organizația Europeană de Brevete este invitată să informeze Comisia cu privire la evoluțiile semnificative relevante pentru prezenta decizie în ceea ce privește prelucrarea datelor cu caracter personal și limitările și garanțiile aplicabile accesului autorităților publice la datele cu caracter personal.

(108) În plus, pentru a permite Comisiei să își exercite în mod eficace funcția de monitorizare, statele membre ar trebui să informeze Comisia cu privire la orice acțiune relevantă întreprinsă de autoritățile naționale pentru protecția datelor, în special în ceea ce privește solicitările sau plângerile formulate de persoane vizate din Uniune cu privire la transferul de date cu caracter personal din Uniune către Organizația Europeană de Brevete.

(109) În conformitate cu articolul 45 alineatul (3) din Regulamentul (UE) 2016/679 și având în vedere faptul că nivelul de protecție asigurat de cadrul juridic al Organizației Europene de Brevete poate suferi modificări, Comisia, în urma adoptării prezentei decizii, ar trebui să verifice periodic dacă respectivele constatări referitoare la caracterul adecvat al nivelului de protecție asigurat de Organizația Europeană de Brevete sunt în continuare justificate în fapt și în drept. Astfel de evaluări ar trebui să aibă loc cel puțin o dată la patru ani și ar trebui să acopere toate aspectele legate de funcționarea prezentei decizii, inclusiv funcționarea mecanismelor relevante de supraveghere și de asigurare a respectării legii.

(110) Pentru a efectua această revizuire, ar trebui să se organizeze o reuniune între Comisie și Organizația Europeană de Brevete, cu participarea responsabilului cu protecția datelor și a Comitetului pentru protecția datelor. Participarea la reuniunea respectivă ar trebui să fie deschisă reprezentanților membrilor Comitetului european pentru protecția datelor. În cadrul revizuirii, Comisia ar trebui să solicite Organizației Europene de Brevete să furnizeze informații cuprinzătoare cu privire la toate aspectele relevante pentru constatarea referitoare la caracterul adecvat. Comisia ar trebui, de asemenea, să solicite explicații cu privire la orice informație relevantă pentru prezenta decizie pe care a primit-o, inclusiv din partea CEPD, a autorităților individuale pentru protecția datelor și a grupurilor societății civile, precum și din cadrul rapoartelor publice sau ale mass-mediei sau din orice altă sursă de informații disponibilă.

(111) Pe baza revizuirii, Comisia ar trebui să pregătească un raport public, care să fie prezentat Parlamentului European și Consiliului.

(112) În cazul în care informațiile disponibile, în special informațiile rezultate din monitorizarea de către Comisie a evoluțiilor care ar putea afecta funcționarea prezentei decizii în temeiul articolului 45 alineatul (4) din Regulamentul (UE) 2016/679 sau furnizate de Organizația Europeană de Brevete sau de autoritățile statelor membre, arată că nivelul de protecție oferit de Organizația Europeană de Brevete ar putea să nu mai fie adecvat, Comisia ar trebui să informeze Organizația Europeană de Brevete în acest sens și să solicite luarea unor măsuri adecvate într-un termen rezonabil specificat.

(113) În cazul în care, la expirarea termenului specificat, Organizația Europeană de Brevete nu ia măsurile respective sau nu demonstrează în mod satisfăcător în alt fel că prezenta decizie continuă să se bazeze pe un nivel de protecție adecvat, Comisia va iniția procedura menționată la articolul 93 alineatul (2) din Regulamentul (UE) 2016/679 în vederea suspendării sau a abrogării parțiale sau integrale a prezentei decizii.

([291]) Cauza C-362/14, Schrems („hotărârea Schrems I"), ECLI:EU:C:2015:650, punctul 65.

(114) Ca alternativă, Comisia inițiază această procedură în vederea modificării prezentei decizii, în special prin aplicarea unor condiții suplimentare transferurilor de date sau prin limitarea domeniului de aplicare al constatării referitoare la caracterul adecvat numai la transferurile de date pentru care se asigură în continuare un nivel de protecție adecvat.

(115) De asemenea, Comisia ar trebui să aibă în vedere inițierea procedurii care conduce la modificarea, suspendarea sau abrogarea prezentei decizii în cazul în care, în contextul revizuirii sau într-un alt context, Organizația Europeană de Brevete nu furnizează informațiile sau clarificările necesare pentru evaluarea nivelului de protecție acordat datelor cu caracter personal transferate din Uniune către Organizația Europeană de Brevete sau în ceea ce privește respectarea prezentei decizii. În această privință, Comisia ar trebui să ia în considerare măsura în care informațiile relevante pot fi obținute din alte surse.

(116) Din motive imperioase de urgență justificate corespunzător, Comisia va face uz de posibilitatea de a adopta, în conformitate cu procedura menționată la articolul 93 alineatul (3) din Regulamentul (UE) 2016/679, acte de punere în aplicare imediat aplicabile de suspendare, abrogare sau modificare a deciziei.

7. **CONSIDERAȚII FINALE**

(117) Comitetul european pentru protecția datelor și-a publicat avizul ([292]), care a fost luat în considerare la pregătirea prezentei decizii.

(118) Măsurile prevăzute în prezenta decizie sunt conforme cu avizul comitetului instituit în temeiul articolului 93 alineatul (1) din Regulamentul (UE) 2016/679,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

În sensul articolului 45 din Regulamentul (UE) 2016/679, Organizația Europeană de Brevete asigură un nivel de protecție adecvat pentru datele cu caracter personal transferate din Uniune către Organizația Europeană de Brevete.

Articolul 2

Ori de câte ori autoritățile competente din statele membre, pentru a proteja persoanele fizice în ceea ce privește prelucrarea datelor cu caracter personal, își exercită competențele în temeiul articolului 58 din Regulamentul (UE) 2016/679 în ceea ce privește transferurile de date care intră în domeniul de aplicare prevăzut la articolul 1, statul membru în cauză informează fără întârziere Comisia în acest sens.

Articolul 3

(1) Comisia monitorizează în permanență aplicarea cadrului juridic al Organizației Europene de Brevete pe care se bazează prezenta decizie pentru a evalua dacă Organizația Europeană de Brevete continuă să asigure un nivel de protecție adecvat în sensul articolului 1.

(2) Statele membre și Comisia se informează reciproc cu privire la cazurile în care Organizația Europeană de Brevete nu asigură respectarea cadrului juridic pe care se bazează prezenta decizie.

(3) Cel puțin o dată la patru ani, Comisia evaluează constatarea menționată la articolul 1 pe baza tuturor informațiilor disponibile, inclusiv a informațiilor primite în cadrul revizuirii realizate împreună cu Organizația Europeană de Brevete.

([292]) Comitetul european pentru protecția datelor, 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. Disponibil la adresa: https://www.edpb.europa.eu/system/files/2025-05/edpb-opinion-202507-epo-adequacydecision_en.pdf.

(4) În cazul în care Comisia dispune de indicii potrivit cărora nu mai este asigurat un nivel de protecție adecvat, aceasta informează Organizația Europeană de Brevete în acest sens. Dacă este necesar, Comisia poate decide să suspende, să modifice sau să abroge prezenta decizie ori să limiteze domeniul de aplicare al acesteia, în conformitate cu articolul 45 alineatul (5) din Regulamentul (UE) 2016/679.

Comisia poate, de asemenea, să suspende, să abroge sau să modifice prezenta decizie în cazul în care lipsa de cooperare a Organizației Europene de Brevete o împiedică să stabilească dacă este afectată evaluarea menționată la articolul 1 din prezenta decizie.

Articolul 4

Prezenta decizie se adresează statelor membre.

Adoptată la Bruxelles, 15 iulie 2025.

Pentru Comisie
Michael MCGRATH
Membru al Comisiei