2025/1382

18.7.2025

DECISIONE DI ESECUZIONE (UE) 2025/1382 DELLA COMMISSIONE

del 15 luglio 2025

a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sulla protezione adeguata dei dati personali da parte dell'Organizzazione europea dei brevetti

[notificata con il numero C(2025) 4626]

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) ([1]), in particolare l'articolo 45, paragrafo 3,

considerando quanto segue:

1. INTRODUZIONE

(1) Il regolamento (UE) 2016/679 stabilisce le norme per il trasferimento di dati personali da titolari del trattamento o responsabili del trattamento nell'Unione verso paesi terzi e organizzazioni internazionali, nella misura in cui tale trasferimento rientri nel suo ambito di applicazione. Le norme sui trasferimenti internazionali di dati sono stabilite nel capo V (articoli da 44 a 50) di detto regolamento. Sebbene la circolazione di dati personali verso e da paesi e organizzazioni internazionali al di fuori dell'Unione sia essenziale per l'espansione degli scambi transfrontalieri e della cooperazione internazionale, occorre garantire che il livello di protezione offerto ai dati personali nell'Unione non sia compromesso dai trasferimenti verso paesi terzi e organizzazioni internazionali ([2]).

(2) Ai sensi dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 la Commissione può decidere, mediante atti di esecuzione, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato. Nel rispetto di tale condizione, i trasferimenti di dati personali verso un'organizzazione internazionale possono avvenire senza la necessità di ottenere ulteriori autorizzazioni, come previsto dall'articolo 45, paragrafo 1, e illustrato dal considerando 103 del richiamato regolamento.

(3) Come specificato all'articolo 45, paragrafo 2, del regolamento (UE) 2016/679, l'adozione di una decisione di adeguatezza deve basarsi su un'analisi completa del regime giuridico dell'organizzazione internazionale, per quanto riguarda tanto le norme applicabili agli importatori di dati quanto le limitazioni e le garanzie relative all'accesso ai dati personali da parte delle autorità pubbliche. Nella propria valutazione la Commissione deve stabilire se l'organizzazione internazionale in questione assicura un livello di protezione «sostanzialmente equivalente» a quello garantito all'interno dell'Unione ([3]). Il criterio rispetto al quale viene valutata l'«equivalenza sostanziale» è quello stabilito dalla legislazione dell'Unione, in particolare il regolamento (UE) 2016/679, nonché dalla giurisprudenza della Corte di giustizia dell'Unione europea ([4]). Anche i «criteri di riferimento per l'adeguatezza» del comitato europeo per la protezione dei dati (EDPB) sono importanti al riguardo, al fine di chiarire ulteriormente tale criterio e fornire orientamenti ([5]).

([1]) GU L 119 del 4.5.2016, pag. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.
([2]) Cfr. considerando 101 del regolamento (UE) 2016/679.
([3]) Cfr. considerando 104 del regolamento (UE) 2016/679.
([4]) Cfr. sentenza della Corte di giustizia del 16 luglio 2020, *Facebook Ireland e Schrems* («Schrems II»), C-311/18, ECLI:EU:C:2020:559, punto 94.
([5]) Comitato europeo per la protezione dei dati, Criteri di riferimento per l'adeguatezza, WP 254 rev. 01, disponibile all'indirizzo https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

(4) Come chiarito dalla Corte di giustizia, un paese terzo o un'organizzazione internazionale non può essere tenuto ad assicurare un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione ([6]). In particolare gli strumenti dei quali il paese terzo o l'organizzazione internazionale in questione si avvale per proteggere i dati personali possono essere diversi da quelli attuati all'interno dell'Unione, purché si rivelino efficaci, nella prassi, al fine di assicurare un livello di protezione adeguato ([7]). Il livello di adeguatezza non comporta pertanto una riproduzione pedissequa delle norme dell'Unione. Si tratta piuttosto di determinare se il sistema straniero nel suo insieme, tramite il contenuto essenziale dei diritti alla riservatezza e delle garanzie in materia di protezione dei dati (compresi l'attuazione, l'azionabilità e il controllo effettivi), nonché tramite le circostanze relative ad un trasferimento di dati personali, offre il necessario livello di protezione ([8]).

(5) La Commissione ha analizzato il quadro giuridico e la prassi dell'Organizzazione europea dei brevetti. Sulla base delle risultanze illustrate nei considerando da 7 a 100, la Commissione conclude che l'Organizzazione europea dei brevetti assicura un livello di protezione adeguato per i dati personali trasferiti dall'Unione all'Organizzazione stessa nell'ambito di applicazione del regolamento (UE) 2016/679.

(6) Ai sensi della presente decisione, i trasferimenti dai titolari del trattamento e dai responsabili del trattamento nell'Unione all'Organizzazione europea dei brevetti possono avvenire senza la necessità di ottenere ulteriori autorizzazioni. La presente decisione non dovrebbe incidere sull'applicazione diretta del regolamento (UE) 2016/679 a tali soggetti qualora siano soddisfatte le condizioni relative all'ambito di applicazione territoriale di cui all'articolo 3 di detto regolamento.

2. NORME CHE SI APPLICANO AL TRATTAMENTO DEI DATI PERSONALI

2.1. Organizzazione e compiti dell'Organizzazione europea dei brevetti

(7) L'Organizzazione europea dei brevetti (OEB) è un'organizzazione intergovernativa che è stata istituita il 7 ottobre 1977 sulla base della convenzione sul brevetto europeo (CBE). L'OEB ha sede a Monaco di Baviera e conta 39 Stati contraenti, tra cui tutti gli Stati membri dell'Unione, l'Islanda, la Norvegia e il Liechtenstein, nonché l'Albania, la Macedonia del Nord, Monaco, San Marino, la Serbia, la Svizzera, il Montenegro, il Regno Unito e la Turchia ([9]).

(8) L'OEB è dotata di personalità giuridica ([10]) ed è composta da due organi ([11]): l'Ufficio europeo dei brevetti (Ufficio) e il Consiglio d'amministrazione. Il compito principale dell'OEB è il rilascio di brevetti europei ([12]) conformemente alla CBE, che è effettuato dall'Ufficio sotto il controllo del Consiglio d'amministrazione. Il Consiglio d'amministrazione si compone dei rappresentanti degli Stati contraenti ed esercita poteri legislativi per conto dell'OEB. È inoltre responsabile delle questioni in materia di politiche e supervisiona le attività dell'Ufficio ([13]). L'Ufficio, che funge da braccio esecutivo dell'OEB, è guidato da un Presidente ([14]) che gestisce l'Ufficio e risponde al Consiglio d'amministrazione ([15]). Il Presidente, tra l'altro, prepara ed esegue il bilancio dell'Ufficio, nomina e supervisiona il personale dell'Ufficio, esercita il potere disciplinare sul personale, garantisce il funzionamento dell'Ufficio, comprese

([6]) Sentenza della Corte di giustizia del 6 ottobre 2015, *Schrems* («Schrems I»), C-362/14, ECLI:EU:C:2015:650, punto 73.
([7]) Schrems I, punto 74.
([8]) Schrems I, punto 75.
([9]) Il numero corrisponde a quello degli Stati contraenti a febbraio 2025.
([10]) Articolo 5, paragrafo 1, CBE.
([11]) Articolo 4, paragrafo 2, CBE.
([12]) In ciascuno degli Stati contraenti per i quali esso è concesso, il brevetto europeo ha, in linea di principio, gli stessi effetti ed è soggetto alle medesime regole di un brevetto nazionale concesso in questo Stato (cfr. articolo 2, paragrafo 2, CBE).
([13]) Articoli 26 e 33 CBE.
([14]) Il Presidente è nominato dal Consiglio d'amministrazione e rappresenta l'OEB esternamente (articolo 5, paragrafo 3, CBE).
([15]) Articolo 10, paragrafo 1, CBE.

l'adozione di norme amministrative interne e la pubblicazione di comunicazioni destinate al pubblico, e può sottoporre al Consiglio d'amministrazione proposte di modifica della convenzione, di regolamenti generali o di decisioni che sono di competenza del Consiglio d'amministrazione ([16]). L'Ufficio è composto da diversi servizi, tra cui una sezione di deposito, una divisione giuridica, divisioni di esame e d'opposizione e le commissioni di ricorso (un organo interno indipendente dinanzi al quale possono essere impugnate le decisioni adottate dall'OEB nell'ambito della procedura di rilascio dei brevetti) ([17]).

(9) Nello svolgimento dei suoi compiti, l'OEB riceve dati personali da diversi attori nell'Unione. Su base continuativa, le domande di brevetto europeo ([18]) sono depositate presso l'OEB dai richiedenti o trasmesse all'OEB dagli uffici nazionali dei brevetti degli Stati membri ([19]). L'OEB riceve e tratta dati personali anche nel contesto dei compiti ad essa affidati a norma del regolamento (UE) n. 1257/2012 del Parlamento europeo e del Consiglio ([20]). Tali compiti comprendono il ricevimento e l'esame delle richieste di effetto unitario dei brevetti europei, la riscossione di tasse annuali e la registrazione dell'effetto unitario ([21]). In tale contesto, l'OEB riceve anche richieste dal tribunale unificato dei brevetti su ricorsi in corso dinanzi alla commissione di ricorso dell'Ufficio ([22]), che possono includere dati personali necessari per individuare il caso in questione ([23]).

(10) Analogamente, l'OEB riceve i dati personali contenuti nelle domande di brevetto internazionali quando agisce ai sensi del trattato di cooperazione in materia di brevetti (TCB), un trattato internazionale che consente ai richiedenti di ottenere brevetti con effetti in tutti gli Stati contraenti del trattato medesimo ([24]). L'OEB agisce in qualità di amministrazione incaricata della ricerca internazionale nell'ambito del TCB e, in tale veste, esamina la brevettabilità delle invenzioni divulgate nelle domande internazionali, il che aiuta i richiedenti a decidere se presentare o meno una domanda di esame nel merito a livello nazionale/dell'Unione ([25]).

(11) Inoltre l'OEB coopera strettamente con gli uffici nazionali dei brevetti di tutti gli Stati membri nel contesto di una «rete europea dei brevetti» e, in tale contesto, scambia con loro dati personali, ad esempio quando fornisce corsi di formazione e servizi informatici per sostenere e rafforzare la cooperazione nell'ambito della CBE. Analogamente, ha concluso accordi di cooperazione bilaterale con gli Stati membri che prevedono lo scambio di dati personali, ad esempio nel contesto dell'istituzione di gruppi di lavoro, del distacco e dell'invio di esperti tecnici ecc. Essa collabora inoltre strettamente con l'Ufficio dell'Unione europea per la proprietà intellettuale (EUIPO), ad esempio organizzando corsi di formazione congiunti ed eventi di sensibilizzazione e distaccando esperti.

([16]) Articolo 10, paragrafo 2, CBE.

([17]) I membri delle commissioni di ricorso sono nominati dal Consiglio d'amministrazione (su proposta del Presidente) e operano in modo indipendente (articolo 11, paragrafo 3, e articolo 23 CBE).

([18]) Esse comprendono, ad esempio, il nome, l'indirizzo, la cittadinanza e il numero di telefono dei richiedenti; il nome e l'indirizzo degli inventori e dei mandatari in materia di brevetti; il nome e le informazioni finanziarie della persona che effettua i pagamenti ecc. L'OEB può ottenere dati personali supplementari se terzi si oppongono al rilascio di un brevetto, nel qual caso informazioni supplementari, quali osservazioni, prove e dichiarazioni scritte di terzi, possono essere condivise con l'OEB (cfr. il regolamento di esecuzione della CBE, ad esempio Rule 41, paragrafo 2, Rule 143, paragrafo 1, lettera h), Rule 92, paragrafo 2, lettera c), Rule 19, paragrafo 1, Rule 53, paragrafo 1 ecc.). Cfr. anche l'articolo 9 della decisione del Presidente sulla procedura di concessione del brevetto.

([19]) Una domanda di brevetto europeo può essere depositata presso l'ufficio centrale della proprietà industriale o un'altra autorità competente di uno Stato contraente. Dopo aver verificato la domanda in relazione ai requisiti di sicurezza o ad altri requisiti nazionali, l'autorità nazionale la trasmette all'OEB.

([20]) Regolamento (UE) n. 1257/2012 del Parlamento europeo e del Consiglio, del 17 dicembre 2012, relativo all'attuazione di una cooperazione rafforzata nel settore dell'istituzione di una tutela brevettuale unitaria (GU L 361 del 31.12.2012, pag. 1, ELI: http://data.europa.eu/eli/reg/2012/1257/oj).

([21]) I brevetti unitari con effetto unitario per tutti gli Stati membri partecipanti sono registrati a livello centrale presso l'OEB, senza che siano necessarie ulteriori misure amministrative a livello nazionale (come richiesto per i brevetti europei).

([22]) Nel dicembre 2024 l'OEB ha adottato una norma su un meccanismo di controllo indipendente per il trattamento dei dati personali da parte della commissione di ricorso nell'esercizio delle sue funzioni giurisdizionali. Disponibile all'indirizzo https://www.epo.org/en/about-us/transparency-portal?search_description=CA%2FD+19%2F24&op=&sort_by=most&items_per_page=10.

([23]) Il tribunale unificato dei brevetti è stato istituito sulla base dell'accordo su un tribunale unificato dei brevetti (GU C 175 del 20.6.2013, pag. 1) e ha competenza esclusiva per quanto riguarda, tra l'altro, i brevetti europei (fatto salvo un periodo transitorio) e i brevetti europei con effetto unitario (ad esempio per quanto riguarda le azioni per violazione o minaccia di violazione e i relativi controricorsi, le azioni di accertamento di non violazione, le azioni per misure provvisorie e cautelari e ingiunzioni, le azioni di revoca e le domande riconvenzionali di revoca). Il tribunale unificato dei brevetti ha inoltre competenza esclusiva per quanto riguarda le decisioni dell'OEB nello svolgimento dei suoi compiti in materia di tutela brevettuale unitaria.

([24]) Per una panoramica della procedura prevista dal TCB, cfr. «The PCT Applicant's Guide – Introduction to the International Phase», disponibile all'indirizzo https://www.wipo.int/pct/en/guide/index.html, in particolare il capitolo 3, e la «Guide for applicants: PCT procedure before the EPO (Euro-PCT Guide)», 16ª edizione, 1° gennaio 2023, disponibile all'indirizzo https://www.epo.org/en/legal/guide-europct/
2023/index.html. Per le categorie di dati personali trattati dall'OEB nell'ambito di una procedura ai sensi del TCB si veda, in particolare, la sezione 9, lettere a), d), h), i), j), l), m), n) e p), dell'allegato del documento «Decision of the President of the European Patent Office dated 13 December 2021 concerning the processing of personal data in patent-grant and related proceeding» (GU Ufficio europeo dei brevetti 2021, A98).

([25]) Inoltre, in questo caso, una domanda di brevetto potrebbe dover essere trasferita dall'ufficio centrale della proprietà industriale o da un'altra autorità competente di uno Stato contraente del TCB all'OEB.

(12) Infine l'OEB ha contratti con diversi prestatori di servizi dell'Unione che agiscono in qualità di responsabili del trattamento ai sensi dell'articolo 4, punto 8), del regolamento (UE) 2016/679 e trasferiscono dati personali all'OEB.

2.2. **Quadro giuridico applicabile e norme in materia di protezione dei dati**

(13) Il diritto primario che disciplina le attività dell'OEB è istituito da un trattato internazionale, vale a dire la convenzione sul brevetto europeo e, quando l'OEB agisce in forza del trattato di cooperazione in materia di brevetti, da quest'ultimo. A un secondo livello della gerarchia delle norme applicabili all'OEB si trovano gli atti giuridici adottati dal Consiglio d'amministrazione o, per quanto riguarda il TCB, dall'Assemblea del TCB. Il diritto derivato dell'OEB comprende il regolamento di esecuzione della CBE e il cosiddetto statuto (che disciplina gli aspetti relativi al personale dell'OEB, compresi i diritti e gli obblighi del personale) ([26]). Il diritto alla protezione dei dati personali è sancito dall'articolo 1 ter dello statuto ([27]), che contiene anche alcune disposizioni fondamentali del quadro in materia di protezione dei dati dell'OEB, relative all'ambito di applicazione di tale quadro, alla protezione di categorie particolari di dati e all'esercizio dei diritti da parte delle persone fisiche. L'articolo 2, paragrafo 1, e l'articolo 32 bis dello statuto istituiscono meccanismi di vigilanza indipendenti (il responsabile della protezione dei dati (DPO) e il comitato per la protezione dei dati (DPB)) per controllare il rispetto delle norme in materia di protezione dei dati ([28]).

(14) Le stesse condizioni sostanziali che disciplinano la protezione dei dati personali si applicano al Consiglio d'amministrazione e all'Ufficio, nonché a tutti i loro servizi. In particolare, il trattamento dei dati personali da parte dell'Ufficio è disciplinato dal documento «Implementing Rules for Articles 1B and 32A of the Service Regulations for Permanent and Other Employees of the European Patent Office on the Protection of Personal Data» (Data Protection Rules (DPR)), adottato dal Consiglio d'amministrazione ([29]). Il trattamento dei dati personali da parte del Consiglio d'amministrazione è soggetto al documento «Administrative Council Data Protection Rules» (AC DPR), che applica le DPR mutatis mutandis ([30]). Nei casi in cui la presente decisione fa riferimento alle DPR, i riferimenti comprendono le prescrizioni corrispondenti che si applicano al Consiglio d'amministrazione, alla sua segreteria e ai suoi comitati. La struttura e il contenuto delle DPR sono strettamente allineati al quadro dell'Unione in materia di protezione dei dati ([31]). In particolare, molti aspetti comuni sono condivisi con il regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([32]), che stabilisce requisiti in materia di protezione dei dati per le istituzioni e gli organi dell'Unione ed è pertanto adatto alla struttura e alle caratteristiche specifiche delle organizzazioni internazionali, rispecchiando al contempo strettamente il regolamento (UE) 2016/679.

([26]) Articolo 33 CBE.

([27]) Cfr. in particolare l'articolo 1 ter, paragrafo 1, dello statuto, a norma del quale «l'Ufficio si adopera per garantire il rispetto dei diritti fondamentali alla vita privata e alla protezione dei dati personali di tutte le persone i cui dati sono trattati dall'Ufficio e per garantire l'assunzione di responsabilità a tale riguardo". Cfr. anche l'articolo 1, paragrafo 1, delle DPR, che spiega che le DPR forniscono il quadro giuridico necessario per garantire «il rispetto dei diritti fondamentali delle persone fisiche alla vita privata e alla protezione dei loro dati personali trattati dall'Ufficio».

([28]) Cfr. anche articoli 47 e 48 DPR.

([29]) «Data Protection Rules» (pag. 495), disponibile all'indirizzo https://report-archive.epo.org/files/babylon/service_regulations_en.pdf. Le DPR si applicano anche alle commissioni di ricorso dell'Ufficio, ad eccezione della procedura di ricorso dinanzi al comitato per la protezione dei dati, che non si applica al trattamento dei dati personali da parte delle commissioni nell'esercizio delle loro funzioni giurisdizionali (articolo 2, paragrafo 6, DPR). Per tali attività, le DPR impongono alle commissioni di istituire un meccanismo di riesame indipendente distinto.

([30]) «Administrative Council Data Protection Rules», disponibili all'indirizzo https://link.epo.org/ac-document/CA/D%202/23%20-%20En.pdf. L'unico aspetto sul quale le AC DPR differiscono dalle DPR riguarda gli adeguamenti all'assetto specifico del Consiglio d'amministrazione, vale a dire la sostituzione dei riferimenti al Presidente con riferimenti al Presidente del Consiglio d'amministrazione. Inoltre, per il cosiddetto Comitato ristretto del Consiglio d'amministrazione sono state adottate norme distinte, le «Select Committee Data Protection Rules» (SC DPR). Tale Comitato è composto dagli Stati contraenti dell'OEB e dalle organizzazioni di utenti ed è stato istituito dall'articolo 9, paragrafo 2, del regolamento (UE) n. 1257/2012 e dall'articolo 145 CBE per controllare le attività dell'Ufficio nel contesto della procedura brevettuale unitaria. Le SC DPR applicano le AD DPR (che a loro volta applicano le DPR) al trattamento dei dati personali da parte del Comitato ristretto (cfr. https://link.epo.org/web/about-us/governance/SC_D_1_23_en.pdf). Anche in questo caso, le SC DPR differiscono dalle AC DPR solo nel riferimento al Presidente del Comitato (anziché al Presidente del Consiglio o al Presidente).

([31]) «Data Protection Rules» dell'OEB: https://www.epo.org/en/about-us/office/data-protection-and-privacy.

([32]) Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(15) Per quanto riguarda il trattamento dei dati da parte dell'Ufficio, il Presidente ha emanato ulteriori strumenti giuridicamente vincolanti, quali circolari, decisioni e istruzioni amministrative interne ([33]). In particolare, le DPR sono integrate dai documenti «Decision of the President of the European Patent Office dated 13 December 2021 concerning the processing of personal data in patent-grant and related proceeding» (decisione PGP ([34])); «Decision of the President of the European Patent Office dated 7 December 2022 concerning the processing of personal data in proceedings related to European patents with unitary effect» (decisione UP) ([35]); «Decision of the President of the European Patent Office of 17 November 2022 concerning countries and entities considered to ensure adequate protection of personal data» ([36]); «Decision of the President of the European Patent Office dated 2 maggio 2024 identifying the operational units of the Office acting as delegated controllers within the meaning of the Data Protection Rules» ([37]); e «Circular No. 420 Implementing Article 25 of the Data Protection Rules» (circolare n. 420) ([38]). Per quanto riguarda specificamente il trattamento dei dati nell'ambito delle procedure di rilascio dei brevetti, è importante osservare che le prescrizioni in materia di trattamento dei dati personali previste direttamente dalla CBE e dal TCB prevalgono sulle DPR. L'interazione tra CBE e TCB, da un lato, e le DPR, dall'altro, è chiarita nella decisione PGP ([39]) e nella decisione UP. Le prescrizioni specifiche in materia di protezione dei dati derivanti direttamente dalla CBE e dal TCB sono esaminate nei considerando da 55 a 59. Le DPR e i loro strumenti complementari sono giuridicamente vincolanti e applicabili e possono essere invocati dai singoli dinanzi ai meccanismi di ricorso indipendenti, come descritto nei considerando da 89 a 96.

(16) Le norme previste negli strumenti giuridici di cui al considerando 15 sono rese ulteriormente operative in strumenti emessi dal responsabile della protezione dei dati (cfr. considerando da 83 a 88) ([40]), che si applicano al Consiglio d'amministrazione e all'Ufficio, nonché a tutti i loro servizi ([41]).

2.3. **Ambito di applicazione materiale e personale delle DPR**

(17) Ai sensi delle DPR e dello statuto ([42]), tutti i dipendenti dell'OEB sono tenuti a rispettare le DPR quando trattano dati personali. L'ambito di applicazione materiale e personale delle DPR è determinato dai termini «dati personali», «trattamento», «titolare del trattamento», «titolare del trattamento delegato» e «responsabile del trattamento» ivi definiti.

2.3.1. ***Definizione di dati personali e trattamento***

(18) Le definizioni di «dati personali» e di «trattamento» nelle DPR sono identiche a quelle del regolamento (UE) 2016/679 ([43]). Le DPR si applicano a qualsiasi trattamento di dati personali da parte dell'OEB, indipendentemente dal fatto che il trattamento riguardi dati personali dei propri dipendenti o dati di altre persone

([33]) Articolo 10 CBE. Cfr. anche articolo 1, paragrafo 2, lettera a), DPR.
([34]) https://www.epo.org/en/legal/official-journal/2021/12/a98.html. Una decisione analoga, dal titolo «Decision of the President of the Boards of Appeal dated 14 July 2023 concerning the processing of personal data in appeal proceedings before the Boards of Appeal», è stata adottata dal Presidente delle commissioni di ricorso per quanto riguarda il trattamento dei dati nei procedimenti di ricorso dinanzi alle commissioni di ricorso ed è disponibile all'indirizzo https://www.epo.org/en/legal/official-journal/2023/07/a73.html.
([35]) «Decision of the President of the European Patent Office dated 7 December 2022 concerning the processing of personal data in proceedings related to European patents with unitary effect», disponibile all'indirizzo https://www.epo.org/en/legal/official-journal/2022/12/a112.html.
([36]) https://epo.org/en/legal/official-journal/2022/12/a111.html Modificata dalla decisione dell'11 maggio 2023 (GU Ufficio europeo dei brevetti 2023, A57) disponibile all'indirizzo 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 Questa decisione è aggiornata almeno una volta all'anno.
([38]) «Circular No. 420 Implementing Article 25 of the Data Protection Rules», disponibile all'indirizzo https://link.epo.org/web/circular_420_en.pdf.
([39]) Per quanto riguarda il trattamento dei dati personali da parte delle commissioni di ricorso nei procedimenti di ricorso, tale interazione è chiarita nel documento «Decision of the President of the Boards of Appeal dated 14 July 2023 concerning the processing of personal data in appeal proceedings before the Boards of Appeal».
([40]) Cfr. ad esempio il riferimento di cui all'articolo 1, paragrafo 2, lettera c), DPR ai documenti operativi emessi dal DPO che sono stati approvati dal Presidente e sono quindi diventati vincolanti.
([41]) Cfr. articolo 1, paragrafo 6, e articolo 12, paragrafo 5, AC DPR.
([42]) Articolo 2, paragrafo 2, DPR e articolo 1 dello statuto.
([43]) Articolo 3, primo comma, lettere a) e b), DPR e articolo 4, punti 1) e 2), GDPR.

fisiche ([44]). Anche i dati sottoposti a pseudonimizzazione ([45]) sono considerati dati personali, mentre i dati di persone decedute o di persone giuridiche o le informazioni anonime ([46]) non sono trattati come dati personali ai sensi delle DPR ([47]).

(19) Le DPR si applicano al trattamento interamente o parzialmente automatizzato di dati personali da parte dell'OEB e al trattamento non automatizzato di dati personali contenuti in un archivio ([48]) o destinati a figurarvi.

2.3.2. ***Titolare del trattamento, titolare del trattamento delegato e responsabile del trattamento***

(20) Le DPR definiscono il «titolare del trattamento» come «un'entità, vale a dire l'Ufficio europeo dei brevetti, che, da sola o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali» ([49]). In linea di principio, il Presidente agisce in qualità di titolare del trattamento per le operazioni di trattamento dei dati effettuate dall'Ufficio ([50]). Lo stesso vale per il Consiglio d'amministrazione (in cui il Presidente agisce in qualità di titolare del trattamento), le commissioni di ricorso nell'esercizio delle loro funzioni giurisdizionali (in cui il Presidente agisce in qualità di titolare del trattamento ([51])) e il Comitato ristretto (in cui il Presidente agisce in qualità di titolare del trattamento ([52])). Il titolare del trattamento può delegare questo potere a unità operative rappresentate da un dirigente di alto livello ([53]). In tali casi, le unità operative agiscono in qualità di «titolari del trattamento delegati» ([54]) che definiscono la finalità (ad esempio motivo, giustificazione ed esigenze operative), i mezzi di un'operazione di trattamento e garantiscono che tutte le operazioni di trattamento che implicano dati personali siano conformi alle norme delle DPR ([55]). In tali casi, il titolare del trattamento rimane responsabile del trattamento dei dati personali. Le DPR prevedono inoltre uno scenario di «contitolarità del trattamento» in cui un titolare del trattamento determina la finalità e i mezzi del trattamento insieme a uno o più titolari del trattamento al di fuori dell'OEB ([56]).

([44]) Articolo 1 ter, paragrafo 2, dello statuto e articolo 2, paragrafo 2, e articolo 3 DPR. Cfr. anche la definizione di «interessato» (articolo 3, primo comma, lettera w), DPR), vale a dire «qualsiasi persona fisica identificata o identificabile, indipendentemente dal fatto che tale persona sia o meno un dipendente dell'Ufficio». Per stabilire l'identificabilità di una persona si devono considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente.

([45]) Vale a dire «il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile», cfr. articolo 3, primo comma, lettera e), DPR.

([46]) Vale a dire «un'informazione che non riconduce a una persona fisica identificata o identificabile, ovvero dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato», cfr. articolo 3, primo comma, lettera r), DPR. Ai sensi dell'articolo 13, paragrafo 1, DPR, il titolare del trattamento non è tenuto a conservare, acquisire o trattare ulteriori informazioni per identificare una persona fisica al solo fine di rispettare le DPR, qualora le finalità per le quali i dati sono trattati non richiedano o non richiedano più l'identificazione di una persona fisica.

([47]) Articolo 2, paragrafo 4, DPR. Per quanto riguarda il trattamento dei dati personali a fini di archiviazione (nell'esercizio legittimo dei pubblici poteri dell'OEB), di ricerca scientifica o storica o a fini statistici, le DPR richiedono l'adozione di misure tecniche e organizzative, tra l'altro per garantire il rispetto del principio della minimizzazione dei dati e, qualora la finalità del trattamento possa essere conseguita con tale modalità, per trattare i dati in modo tale da non consentire più l'identificazione della persona (articolo 14 DPR).

([48]) Articolo 1 ter, paragrafo 3, dello statuto e articolo 2, paragrafo 1, DPR. Si definisce «archivio» «qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico», cfr. articolo 3, primo comma, lettera f), DPR.

([49]) Articolo 3, paragrafo 1, lettera g), DPR. Ai fini della presente decisione il termine «titolare del trattamento» si riferisce all'OEB stessa o ai titolari del trattamento delegati.

([50]) Articolo 10, paragrafo 2, CBE e articolo 28, paragrafo 1, DPR.

([51]) Articolo 28, paragrafo 2, DPR. Ciò deriva in particolare da una delega di potere del Presidente dell'Ufficio, cfr. https://www.epo.org/en/legal/official-journal/2021/etc/se1/p175.html. Per altre attività (qualora le commissioni non agiscano nell'esercizio delle loro funzioni giurisdizionali), il Presidente delle commissioni agisce in qualità di titolare del trattamento delegato per il Presidente dell'Ufficio.

([52]) Cfr. articolo 1, paragrafi 4 e 5, AC DPR e articolo 13 bis, paragrafo 2, del documento «Rules of Procedure of the Select Committee».

([53]) Articolo 28, paragrafo 3, DPR.

([54]) Cfr. articolo 3, primo comma, lettera h), DPR. La persona che rappresenta l'unità operativa deve essere un dirigente di alto livello, di norma almeno un amministratore principale. L'elenco dei titolari del trattamento delegati è reso pubblico (cfr. ad esempio https://link.epo.org/web/en-decision-of-the-president-on-delegated-controllers.pdf and https://link.epo.org/web/decision_of_the_president_of_the_boards_of_appeal_appointing_a_delegated_controller_en.pdf) ed è aggiornato regolarmente.

([55]) Quando la presente decisione fa riferimento a un «titolare del trattamento», sono compresi i pertinenti titolari del trattamento delegati.

([56]) In tal caso, l'articolo 29 DPR impone al titolare del trattamento (delegato) di determinare, in modo trasparente, le rispettive responsabilità di entrambe le parti per quanto riguarda il rispetto dei loro obblighi in materia di protezione dei dati e in particolare l'esercizio dei diritti delle persone fisiche e gli obblighi di trasparenza.

(21) La definizione di «responsabile del trattamento» nelle DPR è identica a quella di cui all'articolo 4, punto 8), del regolamento (UE) 2016/679, vale a dire la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altra entità che tratta dati personali per conto del titolare del trattamento ([57]). Il titolare del trattamento è autorizzato a ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti che saranno messe in atto misure tecniche e organizzative adeguate per garantire che il trattamento soddisfi le prescrizioni delle DPR ([58]). Il rapporto tra il titolare del trattamento e il responsabile del trattamento deve essere disciplinato da un contratto o da un atto giuridico che vincoli il responsabile del trattamento e in cui siano stipulati, tra l'altro, la materia disciplinata, la durata, la natura e la finalità del trattamento ([59]). Il responsabile del trattamento è autorizzato a trattare i dati soltanto su istruzione documentata del titolare del trattamento. Il responsabile del trattamento è tenuto ad assistere il titolare del trattamento nell'adempimento dei suoi obblighi ai sensi delle DPR. Il responsabile del trattamento non può ricorrere a sub-responsabili del trattamento senza la preventiva autorizzazione del titolare del trattamento ([60]). Un accordo standard sul trattamento dei dati è disponibile per i titolari del trattamento delegati ([61]). Inoltre, se un responsabile del trattamento è ubicato in un paese terzo, qualsiasi condivisione di dati personali con tale responsabile del trattamento deve rispettare anche le prescrizioni delle DPR per i trasferimenti internazionali, come descritto nei considerando da 68 a 73 della presente decisione ([62]).

2.4. **Garanzie, diritti e obblighi**

2.4.1. ***Liceità e correttezza del trattamento***

(22) I dati personali dovrebbero essere trattati in maniera lecita e corretta.

(23) Tali principi generali sono stabiliti all'articolo 4, paragrafo 2, lettera a), DPR in un modo che può essere considerato identico all'articolo 5, paragrafo 1, lettera a), del regolamento (UE) 2016/679.

(24) Il principio di liceità è ulteriormente sviluppato nell'articolo 5 DPR, che elenca le basi giuridiche sulle quali i dati personali possono essere trattati. Tali basi giuridiche sono a) la necessità di svolgere un compito nell'esercizio delle attività ufficiali dell'OEB ([63]) o nell'esercizio legittimo dei pubblici poteri di cui è investito il titolare del trattamento, compreso il trattamento necessario per la gestione e il funzionamento dell'Ufficio ([64]); b) la necessità di rispettare un obbligo giuridico cui è soggetto il titolare del trattamento (ad esempio pubblicare le informazioni menzionate in una domanda di brevetto nel registro europeo dei brevetti) ([65]); c) la necessità di eseguire un contratto di cui l'interessato è parte o di eseguire misure precontrattuali adottate su richiesta dello stesso; d) il consenso dell'interessato; o e) la necessità di salvaguardare gli interessi vitali dell'interessato o di un'altra persona fisica.

([57]) Articolo 3, primo comma, lettera j), DPR.
([58]) Articolo 30, paragrafo 1, DPR.
([59]) Articolo 30, paragrafo 3, DPR.
([60]) Articolo 30, paragrafi 2 e 3, DPR. Il responsabile del trattamento che ricorre a un sub-responsabile del trattamento è (contrattualmente) tenuto a imporre al sub-responsabile del trattamento gli stessi obblighi in materia di protezione dei dati previsti nel contratto tra il titolare del trattamento e il responsabile del trattamento (articolo 30, paragrafo 4, DPR).
([61]) Allegato E del documento «General Conditions of Contract» dell'OEB, https://link.epo.org/web/general_conditions_of_contract_en.pdf.
([62]) Articolo 8, paragrafi 1, 2 e 5, in combinato disposto con l'articolo 9, paragrafo 1, DPR.
([63]) Si tratta dei compiti svolti ai sensi della CBE e del TCB o delle norme adottate su tale base (ad esempio lo statuto), che sono necessari per svolgere i compiti dell'OEB nella procedura di rilascio dei brevetti. Cfr. anche il punto 5, primo trattino, dell'allegato della decisione PGP e le pertinenti disposizioni della CBE, quali le parti IV e V. Per lo svolgimento dei propri compiti nel contesto della procedura di rilascio dei brevetti, l'OEB tratta dati personali per elaborare domande e brevetti; svolgere procedimenti di opposizione; comunicare con le parti del procedimento (e, se del caso, con terzi); mantenere il registro europeo dei brevetti; compilare relazioni e statistiche e scambiare dati con gli Stati contraenti e con l'Organizzazione mondiale della proprietà intellettuale (punto 6 dell'allegato della decisione PGP).
([64]) Ciò riflette i compiti assegnati al Presidente dell'Ufficio per garantire il funzionamento e la gestione efficaci dello stesso. Cfr. ad esempio l'articolo 10 CBE, che descrive i compiti del Presidente per quanto riguarda il personale, i locali (e il relativo accesso) e i mezzi materiali. Tale approccio è in linea con l'articolo 5, paragrafo 1, lettera a), e il considerando 22 del regolamento (UE) 2018/1725. Analogamente, si riferimento ai compiti del Consiglio d'amministrazione ai sensi della CBE, ad esempio definire le norme in materia di pensioni e i regolamenti finanziari, cfr. articolo 33 CBE, Rule 9, paragrafo 2, Rule 12, lettera c) e Rule 122, paragrafo 4, del regolamento di esecuzione della CBE. Per quanto riguarda il Comitato ristretto, si fa riferimento ai compiti di controllo di cui all'articolo 145 CBE. Infine, per le commissioni di ricorso, si fa riferimento ad esempio alla loro competenza a esaminare i ricorsi contro le decisioni di altre parti dell'Ufficio (cfr. articolo 21, paragrafo 1, CBE).
([65]) Cfr. ad esempio la Rule 20 del regolamento di esecuzione della CBE.

(25) Nelle DPR il consenso è definito nello stesso modo di cui al regolamento (UE) 2016/679, ossia come qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento ([66]). Spetta al titolare del trattamento dimostrare che l'interessato ha acconsentito ([67]). Nel valutare se il consenso sia stato liberamente prestato, si dovrebbe tenere conto dell'eventualità che l'esecuzione di un contratto sia condizionata alla prestazione del consenso al trattamento di dati non necessario all'esecuzione di tale contratto ([68]). Il consenso non può essere considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio ([69]). Inoltre, ai fini di un consenso informato, le DPR prevedono che l'interessato sia posto a conoscenza almeno dell'identità del titolare del trattamento e delle finalità del trattamento cui sono destinati i dati personali ([70]). Infine l'interessato ha il diritto di revocare il consenso in qualsiasi momento ([71]).

2.4.2. ***Trattamenti riguardanti categorie particolari di dati***

(26) Garanzie specifiche dovrebbero essere applicate al trattamento di «categorie particolari» di dati.

(27) Le DPR contengono norme specifiche per quanto riguarda il trattamento di categorie particolari di dati personali ([72]), che sono definite nello stesso modo di cui al regolamento (UE) 2016/679, ossia come «dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici ([73]) o dati biometrici ([74]) intesi a identificare in modo univoco una persona fisica e dati relativi alla salute ([75]) o alla vita sessuale o all'orientamento sessuale della persona» ([76]). Ai sensi delle DPR, il trattamento di categorie particolari di dati è in linea di principio vietato, a meno che non si applichi una deroga specifica ([77]).

(28) Le deroghe specifiche elencate all'articolo 11, paragrafo 2, DPR sono simili a quelle di cui all'articolo 9, paragrafi 2 e 3, del regolamento (UE) 2016/679, con alcuni adeguamenti al quadro giuridico in cui opera l'OEB. Il trattamento di categorie particolari di dati personali è consentito solo in circostanze specifiche e limitate ([78]), vale a dire se 1) l'interessato ha prestato il proprio consenso esplicito; 2) il trattamento è necessario per tutelare un interesse vitale di

([66]) Articolo 3, primo comma, lettera m), DPR. Cfr. anche articolo 7, paragrafo 2, DPR.
([67]) Articolo 7, paragrafo 1, DPR.
([68]) Articolo 7, paragrafi 1, 5, 6 e 7, DPR.
([69]) Articolo 7, paragrafo 4, DPR.
([70]) Articolo 7, paragrafo 4, DPR.
([71]) Articolo 7, paragrafo 5, DPR.
([72]) Cfr. ad esempio l'articolo 11 DPR.
([73]) Definiti come «dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione», cfr. articolo 3, primo comma, lettera o), DPR.
([74]) Definiti come «dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici», cfr. articolo 3, primo comma, lettera p), DPR.
([75]) Vale a dire dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute, cfr. articolo 3, primo comma, lettera q), DPR.
([76]) Articolo 11, paragrafo 1, DPR.
([77]) Articolo 11, paragrafi 1 e 2, DPR.
([78]) Le DPR consentono inoltre il trattamento di categorie particolari di dati in scenari specifici che riguardano principalmente il personale dell'OEB e sono pertanto meno pertinenti per i dati trasferiti sulla base della presente decisione. In particolare, possono essere trattate categorie particolari di dati se autorizzate da una disposizione giuridicamente vincolante che si applica all'Organizzazione europea dei brevetti (ad esempio la CBE e gli strumenti adottati dal Consiglio d'amministrazione e dal Presidente, cfr. articolo 3, primo comma, lettera y), DPR), che prevede garanzie adeguate per i diritti fondamentali e gli interessi dell'interessato (articolo 11, paragrafo 2, lettera b), DPR) e che è necessaria ai fini dell'adempimento degli obblighi e dell'esercizio dei diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale. Analogamente, il trattamento può avere luogo se necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria, sulla base del diritto nazionale che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale, cfr. articolo 11, paragrafo 2, lettera g), DPR. Infine il trattamento può essere richiesto per la medicina preventiva o del lavoro, la valutazione della capacità lavorativa di un dipendente, la diagnosi, l'assistenza o terapia sanitaria o sociale, la gestione dei sistemi e servizi sanitari o sociali o per esami e pareri medici, qualora tali dati siano trattati da un professionista della sanità soggetto all'obbligo del segreto professionale o da un'altra persona soggetta a un obbligo equivalente di segretezza (articolo 11, paragrafo 3, DPR).

una persona (qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso); 3) i dati personali sono stati resi manifestamente pubblici dall'interessato; 4) il trattamento è necessario per una finalità specifica connessa all'esercizio delle attività ufficiali dell'OEB o all'esercizio dei legittimi poteri di cui è investito il titolare del trattamento ([79]); o 5) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria.

(29) Oltre alle categorie particolari di dati personali di cui al considerando 27, le DPR prevedono anche tutele specifiche per il trattamento di dati personali relativi alle condanne penali e ai reati, consentendo tale trattamento solo previa consultazione del DPB o qualora il trattamento sia imposto da uno strumento giuridicamente vincolante che prevede garanzie adeguate per i diritti e le libertà delle persone fisiche ([80]).

2.4.3. *Limitazione delle finalità*

(30) I dati personali dovrebbero essere trattati per una finalità specifica e, di conseguenza, dovrebbero essere utilizzati soltanto nella misura in cui l'uso non sia incompatibile con la finalità del trattamento.

(31) Tale principio è garantito dall'articolo 4, paragrafo 2, lettera b), DPR, ai sensi del quale i dati personali devono essere «raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in un modo che non sia incompatibile con tali finalità».

(32) Analogamente al regolamento (UE) 2016/679, le DPR consentono un ulteriore trattamento (indipendentemente dalla compatibilità della finalità dell'ulteriore trattamento con quella originaria) sulla base del consenso esplicito dell'interessato o sulla base delle disposizioni giuridiche applicabili dell'OEB ([81]). In quest'ultimo caso, le DPR richiedono che il trattamento sia una misura necessaria e proporzionata per la salvaguardia di un obiettivo di interesse pubblico generale ([82]).

(33) Qualora l'ulteriore trattamento non si basi sui suddetti due motivi, le DPR stabiliscono gli elementi da prendere in considerazione per valutare la compatibilità della finalità dell'ulteriore trattamento con la finalità per la quale i dati personali sono stati originariamente raccolti ([83]). Tale approccio e i fattori elencati nelle DPR sono identici a quelli di cui all'articolo 6, paragrafo 4, del regolamento (UE) 2016/679 e all'articolo 6 del regolamento (UE) 2018/1725 ([84]).

2.4.4. *Esattezza e minimizzazione dei dati, limitazione della conservazione e sicurezza dei dati*

(34) I dati personali dovrebbero essere esatti e, se necessario, dovrebbero essere aggiornati. Dovrebbero inoltre essere adeguati, pertinenti e non eccessivi rispetto alle finalità per le quali sono trattati; inoltre, in linea di principio, dovrebbero essere conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

(35) Tali principi sono stabiliti all'articolo 4, paragrafo 2, lettere c), d) ed e), DPR nello stesso modo di cui al regolamento (UE) 2016/679.

([79]) Ad esempio, nel contesto dei ricorsi contro un brevetto rilasciato, i dati sensibili potrebbero essere inclusi nelle dichiarazioni dei testimoni o nelle prove presentate. Il trattamento ai sensi di questa disposizione può essere effettuato anche ove sia sostanzialmente necessario per la gestione e il funzionamento dell'Ufficio e per gli obblighi derivanti dall'obbligo di cooperazione dell'OEB con gli Stati contraenti (ad esempio la necessità di trattare le informazioni sanitarie del personale o dei visitatori conformemente ai requisiti imposti dalle autorità sanitarie pubbliche dello Stato ospitante dell'OEB). In ogni caso, lo strumento giuridico su cui si basa il trattamento deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (articolo 11, paragrafo 2, lettera f), DPR).

([80]) Articolo 12 DPR. Un possibile scenario in cui tali dati sarebbero trattati comprende i procedimenti disciplinari relativi a consulenti in materia di brevetti dinanzi alla commissione disciplinare dell'OEB (cfr. ad esempio la lettera A, punto 7, dell'allegato della decisione PGP).

([81]) Articolo 6, paragrafo 2, DPR.

([82]) Ad esempio, la sicurezza dell'Organizzazione; le attività volte a prevenire, indagare, accertare e perseguire reati; i diritti e le libertà altrui, ecc. (cfr. articolo 25, paragrafo 1, DPR).

([83]) Articolo 6, paragrafo 3, DPR.

([84]) In particolare, ogni nesso tra la finalità della raccolta e la finalità dell'ulteriore trattamento previsto; il contesto in cui i dati sono stati raccolti; la natura di dati; e le possibili conseguenze dell'ulteriore trattamento per le persone fisiche, cfr. articolo 6, paragrafo 3, DPR.

(36) I dati personali dovrebbero inoltre essere trattati in maniera da garantirne la sicurezza, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. A tal fine gli operatori economici dovrebbero adottare misure tecniche od organizzative per proteggere i dati personali da possibili minacce. Tali misure dovrebbero essere valutate tenendo conto dello stato dell'arte e dei costi connessi.

(37) La sicurezza dei dati è sancita nel quadro giuridico dell'OEB attraverso il principio di integrità e riservatezza di cui all'articolo 4, paragrafo 2, lettera f), e all'articolo 33 DPR, in modo quasi identico a quello del regolamento (UE) 2016/679. In particolare, le DPR richiedono che sia garantito un livello di sicurezza adeguato al rischio attraverso misure tecniche e organizzative adeguate, tenendo conto dello stato dell'arte, dei costi di attuazione e della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché della probabilità e gravità diverse di eventuali rischi per i diritti e le libertà delle persone fisiche.

(38) Inoltre le DPR contengono prescrizioni specifiche per il trattamento e la notifica di una violazione dei dati ([85]). In primo luogo, il titolare del trattamento è tenuto a notificare una violazione dei dati al DPO senza ingiustificato ritardo (e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza), a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche ([86]). Analogamente, il responsabile del trattamento è tenuto a notificare una violazione al titolare del trattamento senza ingiustificato ritardo ([87]). La notifica deve descrivere in particolare la natura della violazione, le sue probabili conseguenze e le misure adottate o di cui si propone l'adozione per porvi rimedio ([88]). Quando una violazione dei dati è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento è tenuto altresì a comunicare la violazione all'interessato senza ingiustificato ritardo ([89]). La comunicazione all'interessato deve descrivere la natura della violazione dei dati personali con un linguaggio semplice e chiaro ([90]) e non è richiesta se il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un elevato rischio per i diritti e le libertà degli interessati ([91]).

2.4.5. ***Trasparenza***

(39) Gli interessati dovrebbero essere informati dei principali aspetti del trattamento dei dati personali che li riguardano.

(40) Conformemente alle DPR, il titolare del trattamento è tenuto, al momento dell'ottenimento dei dati personali, a fornire alle persone fisiche informazioni, in particolare, sulla sua identità e i suoi recapiti (nonché i recapiti del DPO), sulla finalità del trattamento e sulla relativa base giuridica, sui destinatari o sulle categorie di destinatari, sul fatto che intende trasferire i dati al di fuori dell'OEB, nonché sui diritti applicabili e sulla possibilità di ottenere riparazione ([92]). Lo stesso vale quando i dati personali sono trattati per una finalità diversa da quella per la quale sono stati raccolti ([93]). Entrambi gli obblighi si applicano solo nella misura in cui la persona interessata non disponga ancora delle informazioni ([94]).

(41) Le stesse informazioni devono essere fornite agli interessati quando i dati personali non sono raccolti direttamente presso di loro, unitamente a informazioni supplementari sulla fonte dei dati personali e sulle categorie di dati in questione ([95]). Tali informazioni devono essere fornite entro un termine ragionevole dall'ottenimento dei dati (ma al più tardi entro un mese), in considerazione delle specifiche circostanze in cui i dati sono trattati ([96]). Nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, le stesse informazioni dovrebbero essere fornite al più tardi al momento della prima comunicazione con la persona ([97]). Le informazioni di cui al considerando 40 devono inoltre essere fornite prima di qualsiasi ulteriore trattamento o, qualora sia prevista una comunicazione a un

([85]) Con «violazione dei dati» s'intende «una violazione di sicurezza che comporta in modo accidentale o illecito la distruzione, la perdita, la modifica, la comunicazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque trattati», cfr. articolo 3, primo comma, lettera n), DPR.
([86]) Articolo 34, paragrafo 1, DPR.
([87]) Articolo 34, paragrafo 2, DPR.
([88]) Articolo 34, paragrafi 1 e 3, DPR.
([89]) Articolo 34, paragrafo 6, DPR.
([90]) Articolo 34, paragrafo 6, DPR.
([91]) Articolo 34, paragrafo 8, DPR.
([92]) Articolo 16, paragrafi 1 e 2, DPR.
([93]) Articolo 16, paragrafo 3, DPR.
([94]) Articolo 16, paragrafo 4, DPR.
([95]) Articolo 17, paragrafi 1 e 2, DPR.
([96]) Articolo 17, paragrafo 3, lettera a), DPR.
([97]) Articolo 17, paragrafo 3, lettera b), DPR.

altro destinatario, al più tardi quando i dati personali sono comunicati a terzi ([98]). Tale obbligo non si applica in una serie di casi, in particolare quando l'interessato dispone già delle informazioni in questione; qualora tali informazioni debbano rimanere riservate a causa di un obbligo di segreto professionale disciplinato sulla base della CBE e/o di altre disposizioni giuridiche applicabili all'OEB ([99]); se la comunicazione di tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato, in particolare per il trattamento a fini di archiviazione, di ricerca scientifica o storica o a fini statistici, nella misura in cui renderebbe impossibile o pregiudicherebbe gravemente il conseguimento delle finalità del trattamento; o qualora l'ottenimento o la divulgazione di tali informazioni sia espressamente previsto dalla CBE o da altre disposizioni giuridiche applicabili che prevedono misure adeguate per tutelare i legittimi interessi dell'interessato ([100]).

2.4.6. ***Diritti delle persone fisiche***

(42) Gli interessati dovrebbero disporre di determinati diritti azionabili nei confronti del titolare del trattamento o del responsabile del trattamento, in particolare il diritto di accesso ai dati, il diritto di rettifica, il diritto di opporsi al trattamento e il diritto di far cancellare i dati. Allo stesso tempo tali diritti possono essere soggetti a limitazioni, purché queste siano necessarie e proporzionate per salvaguardare obiettivi importanti di interesse pubblico generale.

2.4.6.1. *Diritti previsti dalle DPR*

(43) La necessità di agevolare l'esercizio dei diritti individuali è stabilita all'articolo 1 ter, paragrafo 4, dello statuto. Per attuare ulteriormente tale prescrizione, le DPR conferiscono alle persone gli stessi diritti previsti dal regolamento (UE) 2016/679, vale a dire il diritto di accesso (articolo 18 DPR), il diritto di rettifica (articolo 19 DPR), il diritto alla cancellazione (articolo 20 DPR), il diritto di limitazione del trattamento (articolo 21 DPR), il diritto alla portabilità dei dati (articolo 22 DPR), il diritto di opposizione (articolo 23 DPR) e il diritto di non essere sottoposti a un processo decisionale automatizzato (articolo 24 DPR).

(44) Le DPR stabiliscono inoltre disposizioni generali per il trattamento delle richieste di esercizio dei diritti delle persone fisiche, imponendo al titolare del trattamento di comunicare con gli interessati utilizzando un linguaggio semplice e chiaro, in forma concisa, trasparente, intelligibile e facilmente accessibile (per iscritto o con altri mezzi) ([101]). Il titolare del trattamento deve fornire alle persone fisiche informazioni sulle misure adottate in risposta a una richiesta senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa (detto termine può essere prorogato di due mesi, se necessario alla luce della complessità e del numero delle richieste) ([102]). Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può rifiutare di soddisfare la richiesta ([103]). Il titolare del trattamento, se non dà seguito a una richiesta, deve informarne il richiedente e fornire informazioni sulla possibilità di presentare ricorso ([104]).

([98]) Articolo 17, paragrafo 3, lettera c), e paragrafo 4, DPR. All'articolo 3, primo comma, lettera l), DPR, un «terzo» è definito come la persona fisica o giuridica, l'autorità pubblica, il servizio o l'organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile.

([99]) Articolo 17, paragrafo 4, DPR. Tali obblighi di riservatezza si applicano, ad esempio, nel contesto del trattamento di dati personali del personale da parte del servizio medico dell'OEB (nel qual caso i medici interessati possono essere soggetti all'obbligo del segreto professionale, cfr. ad esempio l'articolo 11, paragrafo 3, DPR e il documento «Implementing Rules for Articles 83a, 84 and 84a of the Services Regulation», lettera E) o nel contesto delle procedure di assunzione (sezione 6 dell'allegato II — «Competition Procedures for Posts for which the President of the Office is the Appointing Authority»).

([100]) Vale a dire quando la CBE o gli strumenti giuridici adottati sulle sue basi disciplinano specificamente le informazioni da divulgare ai singoli o al pubblico, cfr. più in dettaglio la sezione 1.4.6.7.

([101]) Articolo 15, paragrafo 1, DPR.

([102]) Articolo 15, paragrafo 2, DPR.

([103]) Articolo 15, paragrafo 4, DPR. Inoltre l'articolo 13, paragrafo 2, DPR chiarisce che, se il titolare del trattamento è in grado di dimostrare di non essere in grado di identificare l'interessato, le disposizioni sui diritti individuali non si applicano (a meno che l'interessato non fornisca ulteriori informazioni che ne consentano l'identificazione).

([104]) Articolo 15, paragrafo 3, DPR.

(45) In primo luogo, per quanto riguarda il diritto di accesso, le DPR conferiscono ai singoli il diritto di ottenere dall'OEB la conferma che i dati personali che li riguardano sono trattati o meno e, in caso affermativo, di accedere facilmente ([105]) e a intervalli ragionevoli a tali dati ([106]). Inoltre le persone fisiche hanno il diritto di ottenere informazioni, in particolare, sulla finalità del trattamento, sulle categorie di dati interessate, sui destinatari con cui i dati sono condivisi e sul periodo previsto per la conservazione dei dati ([107]).

(46) In secondo luogo, le DPR stabiliscono che il diritto di rettifica da esse contemplato consente ai singoli di ottenere la rettifica di dati inesatti o l'integrazione di dati incompleti (ad esempio fornendo una dichiarazione integrativa) ([108]). Una volta effettuata la rettifica, il titolare del trattamento è tenuto a darne comunicazione a ciascun destinatario cui sono stati comunicati i dati personali ([109]). Ai sensi delle DPR, il diritto di rettifica si applica ai dati oggettivi e fattuali e non alle dichiarazioni soggettive ([110]), sebbene in questo caso le persone siano autorizzate a integrare i dati esistenti con un secondo parere o controperizia o a formulare osservazioni ([111]).

(47) In terzo luogo, le DPR conferiscono ai singoli anche un diritto alla cancellazione ([112]), in particolare se a) i dati personali non sono più necessari per le finalità per le quali sono trattati; b) l'interessato revoca il consenso e non sussiste altra base giuridica per il trattamento; c) l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento; d) i dati sono stati trattati illecitamente; o e) i dati devono essere cancellati per adempiere un obbligo legale che si applica al titolare del trattamento ([113]). Il titolare del trattamento deve comunicare eventuali cancellazioni a ciascun destinatario con il quale i dati sono stati condivisi, a meno che ciò non si riveli impossibile o implichi uno sforzo sproporzionato ([114]). Analogamente, il titolare del trattamento, se ha reso pubblici i dati personali, deve adottare misure ragionevoli per informare gli altri titolari del trattamento che stanno trattando tali dati del fatto che la persona fisica ha richiesto la cancellazione ([115]). Il diritto alla cancellazione non si applica alle situazioni seguenti, nella misura in cui il trattamento dei dati sia necessario a) per esercitare il diritto alla libertà di espressione e di informazione; b) per l'adempimento di un obbligo legale dell'OEB o di un obbligo derivante dal dovere dell'OEB di cooperare con i suoi Stati contraenti ([116]) o per l'esercizio di pubblici poteri di cui è investita l'OEB ([117]); c) per motivi di cooperazione con gli Stati contraenti nel settore della sanità pubblica ([118]); d) a fini di archiviazione, di ricerca scientifica o storica e a fini statistici (nella misura in cui la cancellazione rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi del trattamento); o e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria ([119]).

([105]) In particolare, il titolare del trattamento deve fornire una copia in una forma comprensibile dei dati oggetto del trattamento e di tutte le informazioni disponibili (di qualsiasi tipo, indipendentemente dalla loro natura (oggettiva o soggettiva), dal contenuto (compreso qualsiasi tipo di attività svolta) o dal formato (documento cartaceo, registrazioni informatiche, e-mail), cfr. articolo 18, paragrafo 3, DPR. Allo stesso tempo, il diritto di ottenere una copia dei dati non deve ledere i diritti e le libertà altrui (articolo 18, paragrafo 5, DPR).

([106]) Articolo 18, paragrafo 1, DPR.

([107]) Articolo 18, paragrafi 2 e 3, DPR.

([108]) Articolo 19, paragrafo 1, DPR.

([109]) Articolo 19, paragrafo 3, DPR. Se l'interessato lo richiede, il titolare del trattamento deve informare in merito a tali destinatari.

([110]) Tale interpretazione è stata adottata in linea con il documento «Guidelines on the Rights of Individuals with regard to the Processing of Personal Data» del GEPD, disponibile all'indirizzo https://www.edps.europa.eu/sites/default/files/publication/14-02-25_gl_ds_rights_en.pdf. Cfr. in particolare, a pag. 18, gli orientamenti sul diritto di rettifica in relazione a «dati oggettivi e fattuali» e «dichiarazioni soggettive».

([111]) Articolo 19, paragrafo 2, DPR.

([112]) La cancellazione dei dati è definita come «l'eliminazione dei dati conservati in modo tale da renderne impossibile la ricostruzione» (articolo 3, primo comma, lettera v), DPR). Il riferimento ai «dati conservati» comprende tutti i dati raccolti e detenuti dal titolare del trattamento (e da eventuali terzi per conto del titolare del trattamento).

([113]) Articolo 20, paragrafo 1, DPR.

([114]) Articolo 20, paragrafo 4, DPR.

([115]) Articolo 20, paragrafo 2, DPR.

([116]) Ai sensi dell'articolo 20 del documento dell'OEB «Protocol on Privileges and Immunities», l'OEB può essere tenuta a fornire dati personali ai suoi Stati contraenti nell'ambito di procedimenti amministrativi o giudiziari, ad esempio per il calcolo e il trasferimento dei diritti pensionistici del personale, per indagini fiscali, o nell'ambito di processi civili riguardanti il personale dell'OEB.

([117]) Si tratta di situazioni in cui l'OEB è tenuta, conformemente alla CBE, al TCB o agli strumenti giuridici adottati su tale base, a trattare dati personali in relazione alla procedura di rilascio dei brevetti (ad esempio conservando informazioni nel registro europeo dei brevetti e nel bollettino europeo dei brevetti ai sensi degli articoli 127 e 129 CBE).

([118]) Il trattamento dei dati sanitari per motivi di interesse pubblico nel settore della sanità pubblica deve essere conforme all'articolo 11, paragrafo 2, lettera g), DPR.

([119]) Articolo 20, paragrafo 3, DPR.

(48) In quarto luogo, l'articolo 21 DPR prevede un diritto di limitazione del trattamento, vale a dire il contrassegno dei dati personali con l'obiettivo di limitarne il trattamento in futuro (comprese misure di programmazione volte a impedire in modo permanente l'accesso a tali dati) ([120]). Tale diritto può essere invocato in particolare quando la persona fisica contesta l'esattezza dei dati personali (per un periodo richiesto dal titolare del trattamento per verificare l'esattezza) o quando il trattamento è illecito, ma la persona fisica si oppone alla cancellazione dei dati ([121]). Qualora il trattamento sia limitato, i dati personali possono essere trattati, ad eccezione della conservazione, solo con il consenso esplicito della persona fisica, per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, per la tutela dei diritti altrui o per l'esecuzione di un compito svolto nell'esercizio delle attività ufficiali dell'OEB (vale a dire un compito necessario per il lavoro amministrativo e tecnico che l'OEB è tenuta a svolgere conformemente alla CBE) ([122]).

(49) In quinto luogo, un diritto di opposizione è sancito dall'articolo 1 ter, paragrafo 4, dello statuto e dall'articolo 23 DPR. In particolare, i singoli hanno il diritto di opporsi in qualsiasi momento al trattamento di dati personali effettuato per l'esecuzione di un compito nell'esercizio delle attività ufficiali dell'OEB o nell'esercizio legittimo dei pubblici poteri di cui è investito il titolare del trattamento ([123]). I singoli devono essere informati dell'esistenza di tale diritto in modo chiaro e al più tardi al momento della prima comunicazione con loro ([124]). Nel caso in cui un singolo si opponga al trattamento dei dati personali, le DPR impongono al titolare del trattamento di interrompere il trattamento salvo che egli sia in grado di dimostrare l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria ([125]).

(50) In sesto luogo, le DPR istituiscono un diritto alla portabilità dei dati, offrendo alle persone fisiche la possibilità di ricevere i propri dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e di trasmetterli a un altro titolare del trattamento ([126]). Tale diritto si applica quando il trattamento è effettuato con mezzi automatizzati e ha luogo sulla base del consenso della persona fisica o ai fini dell'esecuzione di un contratto con la persona fisica o nell'interesse di quest'ultima ([127]).

(51) Infine, ai sensi delle DPR, i singoli hanno il diritto di non essere sottoposti a un processo decisionale automatizzato, vale a dire una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che li riguardano o che incidono in modo analogo significativamente sulla loro persona ([128]). Le DPR stabiliscono che il processo decisionale automatizzato può avere luogo quando si basa sul consenso esplicito dell'interessato o se è necessario per la conclusione o l'esecuzione di un contratto con la persona fisica, nel qual caso il titolare del trattamento deve attuare garanzie adeguate, ad esempio prevedendo il diritto di ottenere l'intervento umano, di esprimere la propria opinione e di contestare la decisione ([129]). Il processo decisionale automatizzato può essere autorizzato anche da un atto giuridico se tale atto stabilisce misure adeguate per tutelare i diritti delle persone fisiche ([130]). Il titolare del trattamento, se adotta un processo decisionale automatizzato, compresa la profilazione, deve informarne proattivamente la persona nell'ambito dei suoi obblighi di trasparenza e fornire informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato ([131]). Le stesse informazioni devono essere fornite su richiesta ([132]).

([120]) Articolo 3, paragrafo 1, lettera c), DPR.
([121]) Articolo 21, paragrafo 1, DPR.
([122]) Articolo 21, paragrafo 2, DPR.
([123]) Qualora l'OEB sia giuridicamente tenuta a trattare dati personali nell'ambito della procedura di rilascio dei brevetti, vale a dire ai sensi della CBE e del TCB, i singoli non possono opporsi al trattamento, cfr. punto 28 dell'allegato della decisione PGP. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici, gli interessati hanno il diritto, per motivi connessi alla loro situazione particolare, di opporsi al trattamento di dati personali, salvo se il trattamento è necessario per l'esecuzione di un compito svolto nell'esercizio legittimo dei pubblici poteri di cui è investito il titolare del trattamento, compreso il trattamento necessario per la gestione e il funzionamento dell'Ufficio (articolo 23, paragrafo 4, DPR).
([124]) Articolo 23, paragrafo 2, DPR.
([125]) Articolo 23, paragrafo 1, DPR.
([126]) Articolo 22, paragrafo 1, DPR.
([127]) Poiché il trattamento dei dati personali nell'ambito della procedura di rilascio dei brevetti non si basa su nessuno di tali motivi, il diritto alla portabilità dei dati non si applica in tale contesto, cfr. punti 29 e 30 dell'allegato della decisione PGP.
([128]) Articolo 24, paragrafo 1, DPR. La profilazione è definita all'articolo 3, primo comma, lettera d), DPR come qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.
([129]) Articolo 24, paragrafo 3, DPR.
([130]) Articolo 24, paragrafo 2, lettera b), DPR.
([131]) Cfr. l'articolo 16, paragrafo 2, lettera f), e l'articolo 17, paragrafo 2, lettera f), DPR.
([132]) Articolo 18, paragrafo 1, lettera h), DPR.

2.4.6.2. *Limitazioni dei diritti individuali*

(52) Analogamente all'articolo 23 del regolamento (UE) 2016/679 e all'articolo 25 del regolamento (UE) 2018/1725, l'articolo 25 DPR prevede che disposizioni giuridiche specifiche nel quadro giuridico dell'OEB possano limitare l'applicazione dei diritti di cui ai considerando da 43 a 51 ([133]) (ossia limitarne temporaneamente l'applicazione) ([134]), qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali ([135]) e sia una misura necessaria e proporzionata in una società democratica per salvaguardare obiettivi specifici ([136]). Inoltre una limitazione deve essere prevista in disposizioni «chiare e precise» destinate a produrre effetti giuridici nei confronti degli interessati e che devono essere adottate almeno a livello di Presidente ([137]). Tali disposizioni devono, in particolare, stabilire la finalità del trattamento, la portata della limitazione, le garanzie per prevenire abusi, i periodi di conservazione e le garanzie applicabili ([138]).

(53) Attualmente l'unico strumento giuridico che prevede limitazioni dei diritti individuali è la circolare n. 420 (uno strumento giuridicamente vincolante adottato dal Presidente). Essa chiarisce secondo quali modalità e a quali condizioni il titolare del trattamento può applicare limitazioni e stabilisce in modo esaustivo gli scenari specifici in cui i diritti possono essere limitati e per quali obiettivi ([139]). In particolare, prevede che l'OEB possa limitare i diritti individuali per determinati obiettivi specifici: a) e b) quando conduce indagini o procedimenti disciplinari in relazione al suo personale ([140]); c) nel contesto della risoluzione interna delle controversie o dell'accertamento, dell'esercizio o della difesa di un diritto in sede giudiziaria, compreso l'arbitrato, al fine di conservare informazioni e documenti riservati ottenuti dalle parti, dagli intervenienti o da altre fonti legittime; d) quando tratta dati sanitari nelle procedure e nei fascicoli medici, ma solo per tutelare i diritti delle persone ([141]); e) ed f) quando svolge audit e ispezioni interni (queste ultime sono effettuate dal DPO); g) ai fini della gestione degli incidenti informatici e delle relazioni sugli incidenti di sicurezza fisica; e h) quando fornisce o riceve assistenza a o da autorità pubbliche competenti, compresi gli Stati contraenti dell'OEB e le organizzazioni internazionali, o quando coopera con loro ad attività definite nei pertinenti accordi sul livello dei servizi, memorandum d'intesa e accordi di cooperazione, su loro richiesta o su iniziativa dell'Ufficio ([142]).

([133]) Ad eccezione del diritto di opposizione, per il quale la circolare n. 420 non prevede alcuna limitazione, cfr. articolo 3, paragrafo 3. Inoltre, ai sensi dell'articolo 9 della circolare n. 420, l'OEB può limitare la comunicazione di una violazione dei dati a una persona fisica.

([134]) Cfr. la definizione di limitazioni di cui all'articolo 2 della circolare n. 420.

([135]) Non possono essere giustificate limitazioni così ampie e intrusive che, di fatto, privano un diritto fondamentale della sua essenza e impediscono al singolo di esercitare tale diritto, cfr. articolo 4, paragrafo 3, della circolare n. 420.

([136]) Vale a dire la sicurezza dell'OEB, la sicurezza pubblica o la difesa negli Stati contraenti; la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; altri interessi sostanziali dell'OEB relativi alla sua missione principale, o in virtù di obblighi derivanti dal dovere di cooperazione con gli Stati contraenti, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale; la sicurezza interna dell'Ufficio, comprese le sue reti di comunicazione elettronica; la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari e quasi giudiziari; le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate; una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri; la tutela dell'interessato o dei diritti e delle libertà altrui e l'esecuzione delle azioni civili (articolo 25, paragrafo 1, DPR).

([137]) Articolo 25, paragrafo 3, DPR.

([138]) Articolo 25, paragrafo 2, DPR.

([139]) Articolo 1 della circolare n. 420.

([140]) Articolo 4, paragrafo 1, lettere a) e b), della circolare n. 420.

([141]) Ciò riguarda solo il trattamento dei dati sanitari del personale dell'OEB (e non è direttamente pertinente ai fini di una constatazione di adeguatezza riguardante il trattamento dei dati trasferiti da un titolare del trattamento o da un responsabile del trattamento soggetto al GDPR). L'articolo 8 della circolare n. 420 chiarisce ulteriormente le modalità di applicazione delle limitazioni al diritto di accesso ai dati/fascicoli medici. In particolare, specifica che una tale limitazione può essere applicata solo al diritto di accedere direttamente ai dati e/o fascicoli medici personali di natura psicologica o psichiatrica trattati dall'Ufficio, ma solo se l'accesso a tali dati può incidere negativamente sulla vita e la salute dell'interessato o di altri e rappresentare un pericolo immediato in tal senso.

([142]) Articolo 4, paragrafo 1, della circolare n. 420. Questa disposizione riguarda generalmente solo i dati personali del personale dell'OEB. Essa si riferisce ai casi in cui l'OEB è tenuta a cooperare con le autorità nazionali degli Stati contraenti ai sensi dell'articolo 131 CBE (che disciplina la cooperazione tra l'OEB e gli organi giurisdizionali nazionali degli Stati contraenti nelle indagini / nei procedimenti relativi al rilascio di brevetti) e dell'articolo 20, paragrafo 1, del documento «Protocol on Privileges and Immunities» (cfr. anche punto 95). Ciò può verificarsi, ad esempio, quando il personale dell'OEB è invitato a testimoniare dinanzi a un organo giurisdizionale nazionale di uno Stato contraente nell'ambito di un procedimento penale nazionale o quando all'OEB è chiesto di fornire informazioni sulla retribuzione del suo personale in procedimenti civili (di diritto di famiglia) ecc.

(54) La possibilità o meno di applicare una limitazione in un caso specifico deve essere determinata dal titolare del trattamento, nei singoli casi, alla luce delle circostanze pertinenti ([143]). Nel decidere se applicare o meno una limitazione, il titolare del trattamento deve innanzitutto valutarne la necessità e la proporzionalità nel caso specifico, con il coinvolgimento del DPO ([144]). Tale valutazione comporta una ponderazione dei rischi potenziali per i diritti e le libertà dell'interessato rispetto ai rischi e alle libertà di altri interessati e ai rischi di ostacolare la finalità e l'esito dell'operazione di trattamento ([145]). Le limitazioni devono essere documentate, anche registrando la valutazione dei diritti limitati, per quanto tempo, per quali motivi e su quali basi ([146]). Inoltre, finché si applica una limitazione, devono essere messe in atto misure tecniche e organizzative adeguate ([147]). Qualsiasi limitazione può essere applicata solo finché ne sussistono i motivi ([148]). Se un diritto è limitato, il titolare del trattamento deve informare la persona fisica dei principali motivi della limitazione e del diritto di proporre reclamo ([149]).

2.4.6.3. *Norme specifiche nel contesto della procedura di rilascio dei brevetti*

(55) Le disposizioni del trattato costitutivo dell'OEB (vale a dire la CBE) e del TCB e le disposizioni applicabili in virtù di tali trattati (tutte norme di diritto primario dell'OEB) contengono talune prescrizioni specifiche nell'ambito della procedura di rilascio dei brevetti che possono incidere sull'esercizio di determinati diritti ai sensi delle DPR ([150]). La decisione PGP fornisce una panoramica di tali prescrizioni di diritto primario, spiega in che modo i diritti degli interessati possono essere esercitati in tale contesto e stabilisce chiaramente le possibili deroghe ([151]). La circolare n. 420 stabilisce che le disposizioni che possono limitare l'applicazione dei diritti alla protezione dei dati devono indicare chiaramente l'ambito di applicazione di qualsiasi esenzione e quindi bilanciare i diversi interessi in gioco ([152]).

(56) In primo luogo, ai sensi dell'articolo 127 CBE, l'Ufficio ha l'obbligo di tenere un registro europeo dei brevetti, nel quale sono riportati determinati dati personali giuridicamente definiti. Secondo il diritto primario, le domande di brevetto devono essere pubblicate nel corso della procedura di rilascio dei brevetti, in generale, non appena possibile dopo la scadenza del termine di diciotto mesi dalla data di deposito. La CBE prevede che i dati personali contenuti in tali domande di brevetto possano essere consultati mediante consultazione del fascicolo o del registro ([153]). Prima della pubblicazione, le domande di brevetto non possono essere consultate senza il consenso esplicito del richiedente. Norme analoghe sono stabilite nel TCB ([154]).

([143]) Articolo 2 della circolare n. 420.

([144]) Articolo 25, paragrafo 3, lettera a), DPR. Cfr. anche l'articolo 6 della circolare n. 420.

([145]) Articolo 5, paragrafo 5, della circolare n. 420.

([146]) Articolo 4, paragrafo 4, della circolare n. 420. Queste registrazioni devono essere messe a disposizione del DPB su richiesta (articolo 4, paragrafo 7, della circolare n. 420).

([147]) Le misure devono includere, ad esempio, la conservazione sicura, un ambiente elettronico sicuro che impedisca l'accesso illecito e accidentale ai dati elettronici o il loro trasferimento a persone non autorizzate, nonché il controllo delle limitazioni e il riesame periodico della loro applicazione, cfr. articolo 5, paragrafo 2, della circolare n. 420.

([148]) Articolo 4, paragrafo 5, e articolo 5, paragrafo 3, della circolare n. 420.

([149]) Articolo 25, paragrafo 3, lettera b), DPR. Tali informazioni possono essere rinviate, omesse o negate qualora annullino l'effetto della limitazione (cfr. articolo 25, paragrafo 4, DPR). Questa ulteriore limitazione può essere applicata solo in casi debitamente giustificati e per il tempo e nella misura necessari e proporzionati (articolo 7, paragrafo 4, della circolare n. 420). La giustificazione di tale limitazione deve essere riesaminata periodicamente. Oltre all'obbligo specifico di informare le persone in merito a una limitazione dei loro diritti, l'OEB deve fornire informazioni generali sulla propria intranet e/o sul proprio sito web in merito alle attività che possono comportare limitazioni dei diritti (articolo 7, paragrafo 1, della circolare n. 420).

([150]) Articolo 2 della circolare n. 420 («legal provisions of the EPO»).

([151]) Articolo 1 e allegato della decisione PGP.

([152]) Articolo 2 della circolare n. 420.

([153]) Lettera C, punti 13 e 14, dell'allegato della decisione PGP e articolo 128 CBE. Alcune parti dei fascicoli sono escluse dalla consultazione a norma dell'articolo 128, paragrafo 4, della Rule 144 del regolamento di esecuzione della CBE e del documento «Decision of the President of the European Patent Office dated 12 July 2007 concerning documents excluded from file inspection» (edizione speciale n. 3, GU OEB 2007, J.3) Le parti escluse sono le seguenti: i documenti relativi all'esclusione o alla ricusazione di membri delle commissioni di ricorso o della Commissione allargata di ricorso; i progetti di decisioni e di avvisi e tutti gli altri documenti utilizzati per la preparazione di decisioni e avvisi che non sono comunicati alle parti; la designazione dell'inventore, se quest'ultimo ha rinunciato al suo diritto di essere menzionato, e qualsiasi altro documento escluso dalla consultazione da parte del Presidente dell'Ufficio europeo dei brevetti in quanto tale consultazione non avrebbe lo scopo di informare il pubblico in merito alla domanda di brevetto europeo o al brevetto europeo, come ad esempio: certificati medici; richieste di esclusione dalla consultazione del fascicolo e la relativa corrispondenza; informazioni la cui pubblicazione arrecherebbe pregiudizio ai legittimi interessi personali o economici e che non comprendono informazioni rilevanti per la procedura di domanda, di brevetto o di concessione.

([154]) Cfr. l'articolo 3 del documento «Decision of the President of the European Patent Office dated 20 February 2019 concerning online file inspection of documents contained in the file held by the EPO as receiving Office, International Searching Authority or Authority specified for supplementary search» (GU Ufficio europeo dei brevetti 2019, A17). Cfr. a tale proposito l'articolo 30 TCB per quanto riguarda l'accesso del pubblico ai fascicoli, nonché le Rule 48 e 94 TCB. L'OEB invoca tali disposizioni quando agisce in qualità di ufficio o autorità competente ai sensi degli articoli da 151 a 153 CBE.

(57) In secondo luogo, la possibilità di ottenere modifiche delle informazioni utilizzate nell'ambito di una procedura di rilascio di brevetti è specificamente disciplinata dalla CBE ([155]). In particolare, la CBE prevede solo la possibilità di ottenere la correzione di errori nei documenti depositati presso l'OEB ([156]), la correzione di errori nelle decisioni ([157]), la correzione di traduzioni ([158]) e la rettifica della designazione dell'inventore ([159]). La rettifica dei dati personali contenuti nei documenti utilizzati nella procedura di rilascio dei brevetti può quindi essere ottenuta solo in tali casi. Lo stesso vale per la possibilità di ottenere una limitazione del trattamento dei dati ([160]).

(58) In terzo luogo, la CBE impone obblighi specifici di conservazione e pubblicazione per taluni documenti utilizzati nella procedura di rilascio dei brevetti, che incidono sulla possibilità di ottenere la cancellazione delle informazioni ivi contenute, compresi i dati personali ([161]). In particolare, le domande di brevetto pubblicate e le informazioni sui brevetti pubblicate nel bollettino europeo dei brevetti devono essere conservate e messe a disposizione del pubblico ([162]). Di conseguenza, la cancellazione dei dati personali contenuti in tali documenti sarebbe contraria agli obblighi giuridici fondamentali dell'OEB (articolo 129, lettera a), CBE) e non può essere ottenuta. Altri fascicoli devono essere conservati dall'OEB per un periodo specificato nella CBE, che in linea di principio è di cinque anni ([163]). Finché si applica tale termine, le informazioni contenute in tali fascicoli (compresi i dati personali) non possono essere cancellate.

(59) Pertanto, tenuto conto in particolare della loro portata limitata e delle loro condizioni di applicazione, le limitazioni all'esercizio dei diritti derivanti dalle disposizioni di cui ai considerando da 55 a 58 possono essere considerate limitate a quanto necessario e proporzionato per garantire il corretto funzionamento della procedura di rilascio dei brevetti, come richiesto nell'interesse pubblico per l'adempimento dei compiti ufficiali dell'OEB. Nella misura in cui la CBE e il TCB non disciplinano specificamente l'esercizio dei diritti alla protezione dei dati, vale a dire in tutti gli altri scenari diversi da quelli descritti ai considerando da 55 a 58, i requisiti delle DPR si applicano integralmente.

2.4.7. ***Trasferimenti successivi***

(60) Il livello di protezione offerto ai dati personali trasferiti dall'Unione all'OEB non deve essere compromesso da ulteriori trasferimenti di tali dati a destinatari che si trovano in un paese terzo o a un'altra organizzazione internazionale.

(61) Le DPR distinguono tra «trasmissioni di dati personali» (ossia la condivisione di dati da parte dell'OEB con i suoi Stati contraenti) e «trasferimenti di dati personali» (la condivisione di dati da parte dell'OEB con qualsiasi altra persona o entità al di fuori dell'OEB) ([164]).

2.4.7.1. *Trasmissioni di dati*

(62) In primo luogo, le DPR stabiliscono che la trasmissione di dati a un ufficio nazionale per la proprietà intellettuale di uno Stato contraente dell'OEB può aver luogo a) se i dati sono necessari all'esercizio della competenza del destinatario o all'esercizio di pubblici poteri e b) se la trasmissione è necessaria per l'esercizio dei compiti ufficiali/dei pubblici poteri dell'OEB ([165]). Tali trasmissioni si svolgono nell'ambito della procedura di rilascio dei brevetti prevista dalla CBE e dal TCB ([166]).

([155]) Una correzione o una rettifica ai sensi di queste disposizioni può comportare l'aggiornamento delle iscrizioni nel registro europeo dei brevetti e nel bollettino europeo dei brevetti e delle pubblicazioni della domanda o del brevetto. Tuttavia non modificherà retroattivamente il contenuto del fascicolo (che continuerà a contenere tutte le osservazioni delle parti, le comunicazioni e le decisioni dell'OEB), né comporterà la revoca o la soppressione di pubblicazioni precedenti (lettera C, punto 19, dell'allegato della decisione PGP). Ciò vale anche ai sensi degli articoli 19 e 34 TCB, quando l'OEB agisce in qualità di autorità/ufficio competente sulla base degli articoli 151-153 CBE.

([156]) Rule 139 del regolamento di esecuzione della CBE.

([157]) Rule 140 del regolamento di esecuzione della CBE. Nelle decisioni dell'OEB possono essere rettificati unicamente gli errori linguistici o di trascrizione nonché gli errori manifesti.

([158]) Articolo 14, paragrafo 2, seconda frase, CBE.

([159]) Rule 21 del regolamento di esecuzione della CBE. L'errata designazione di un inventore può essere rettificata su richiesta e solo con il consenso della persona erroneamente designata e, se tale richiesta è presentata da un terzo, con il consenso del richiedente o del titolare del brevetto.

([160]) Lettera C, punto 25, dell'allegato della decisione PGP.

([161]) Lettera C, punti 22 e 23, dell'allegato della decisione PGP.

([162]) Articolo 129 CBE.

([163]) Rule 147, paragrafi 4 e 5, del regolamento di esecuzione della CBE.

([164]) Articolo 3, primo comma, lettere s) e t), DPR.

([165]) Articolo 8, paragrafo 2, DPR.

([166]) Cfr. in particolare gli articoli 130, 131 e 135 CBE, nonché il pertinente regolamento di esecuzione della CBE (ad esempio le Rule 148-150). Cfr. anche gli articoli 12, 18, 20 e 36 TCB, nonché le Rule 22, 23, 23 bis, 44, 47 e 71 del regolamento di esecuzione.

(63) In secondo luogo, le DPR consentono la trasmissione di dati a un'autorità pubblica di uno Stato contraente dell'OEB ([167]) qualora i dati siano necessari all'adempimento dei compiti di tale autorità pubblica e la trasmissione sia compatibile con i compiti e il funzionamento dell'OEB ([168]). Tali trasmissioni non sono specificamente richieste dalla CBE o da altri strumenti giuridici che disciplinano la procedura di rilascio dei brevetti, ma possono essere comunque necessarie per lo svolgimento dei compiti dell'OEB, ad esempio la cooperazione dell'OEB con i suoi Stati contraenti attraverso procedure di consultazione; il distacco e l'invio di esperti; o la fornitura di informazioni sul personale dell'OEB ai fini della determinazione delle prestazioni sociali, degli adempimenti fiscali ecc.

(64) Il DPO ha elaborato clausole tipo da includere nei memorandum d'intesa che disciplinano tali trasmissioni descritte ai considerando 62 e 63, che, tra l'altro, prevedono principi di protezione dei dati, limitano l'ulteriore trattamento solo per finalità compatibili, prevedono diritti degli interessati, nonché obblighi in materia di sicurezza dei dati e violazione dei dati e una vigilanza indipendente ([169]).

(65) In entrambi i casi descritti ai considerando 62 e 63, il destinatario, ai sensi delle DPR, deve dimostrare la necessità che i dati siano trasmessi per una finalità specifica derivante dagli obblighi di cooperazione dell'OEB con lo Stato o gli Stati contraenti ([170]). Per ciascuna trasmissione, il titolare del trattamento deve essere in grado di dimostrare che la trasmissione è necessaria e proporzionata alla finalità specifica per la quale sono condivisi i dati ([171]). Qualsiasi trasmissione di dati deve essere effettuata in un modo tale da assicurare che il livello di protezione riconosciuto dalle DPR sia mantenuto ([172]). Secondo gli orientamenti emanati dal DPO, ciò significa che devono essere predisposte garanzie adeguate, anche assicurando che i dati da condividere siano ridotti al minimo e limitati a quanto adeguato, pertinente e strettamente necessario per conseguire tale finalità ([173]). Se vi è motivo di presumere che gli interessi legittimi della persona interessata possano essere lesi, il titolare del trattamento deve dimostrare che è proporzionato trasmettere i dati personali per tale finalità specifica, dopo aver ponderato i diversi interessi in gioco ([174]).

(66) Per quanto riguarda questi due scenari, è altresì importante osservare che tutti gli Stati contraenti dell'OEB sono parte della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, soggetta alla giurisdizione della Corte europea dei diritti dell'uomo, nonché della Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale (STE n. 108).

(67) Infine le DPR consentono la trasmissione di dati a un responsabile del trattamento situato nello Spazio economico europeo (SEE), a condizione che sia garantita la conformità alle prescrizioni stabilite nelle DPR per il coinvolgimento dei responsabili del trattamento ([175]).

2.4.7.2. *Trasferimenti di dati*

(68) La condivisione di dati personali con qualsiasi entità al di fuori dell'OEB diversa da un'autorità pubblica o da un ufficio nazionale per la proprietà intellettuale degli Stati contraenti dell'OEB o da un responsabile del trattamento nel SEE è considerata un «trasferimento» di dati personali, fatte salve le prescrizioni specifiche di cui alle DPR ([176]). Tali prescrizioni si applicano, ad esempio, alla condivisione dei dati con responsabili del trattamento al di fuori del SEE, titolari del trattamento situati in Stati contraenti o al di fuori di essi, amministrazioni pubbliche di Stati non

([167]) Ad esempio, un'autorità nazionale o locale, nonché un altro organismo di diritto pubblico, come un ospedale o un'università.
([168]) Articolo 8, paragrafo 1, DPR.
([169]) «Overview of the requirement of the EPO's model data protection clause for memoranda of understanding», disponibile all'indirizzo https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-template-data-protection-clause-for-mous.pdf.
([170]) Articolo 8, paragrafo 3, DPR.
([171]) Articolo 8, paragrafo 4, DPR.
([172]) Nota esplicativa «EPO transmission and transfer of personal data» (nota sulla trasmissione e il trasferimento), disponibile all'indirizzo https://link.epo.org/web/office/data-protection-and-privacy/en-explanatory-note-on-epo-transmission-and-transfer-of-personal-data.pdf, pag. 4. Si veda in particolare la frase «The EPO DPR […] lay down the general principle of adequate protection, especially applicable to international data stream» («Le DPR dell'OEB [...] stabiliscono il principio generale della protezione adeguata, applicabile soprattutto ai flussi internazionali di dati»).
([173]) Nota sulla trasmissione e il trasferimento, disponibile alla nota 12.
([174]) Articolo 8, paragrafo 3, DPR.
([175]) Articolo 8, paragrafi 1, 2 e 5, DPR.
([176]) Articolo 9, paragrafo 1, DPR.

contraenti e altre organizzazioni internazionali. In generale, le DPR richiedono che il livello di protezione garantito alle persone dall'OEB non sia compromesso quando i dati sono trasferiti a terzi ([177]). Secondo gli orientamenti del DPO, la «protezione accordata ai dati personali trasferiti nel paese terzo o nell'organizzazione internazionale deve essere sostanzialmente equivalente a quella garantita dalle DPR» ([178]).

(69) Ai sensi delle DPR, un trasferimento di dati personali al di fuori dell'OEB può aver luogo innanzitutto se il paese in cui si trova il destinatario, o l'organizzazione internazionale, garantisce un livello di protezione adeguato e se il trasferimento è effettuato unicamente per consentire all'OEB di svolgere compiti di sua competenza ([179]). Una decisione di adeguatezza è adottata dal Presidente ([180]), il quale, in caso di dubbio, decide previa consultazione del DPO e del DPB ([181]). Il DPO ha elaborato «criteri di riferimento per l'adeguatezza» che stabiliscono i criteri per le decisioni di adeguatezza ([182]). In particolare, il quadro giuridico del paese terzo o dell'organizzazione internazionale deve prevedere i principi fondamentali in materia di protezione dei dati, i diritti degli interessati, le norme sui trasferimenti successivi, i meccanismi procedurali e di applicazione e i mezzi di ricorso per le persone fisiche. Se il Presidente adotta una decisione di adeguatezza, il trasferimento può aver luogo senza l'attuazione di garanzie supplementari ([183]). Gli Stati membri, nonché la Norvegia, l'Islanda e il Liechtenstein, tutti i paesi che beneficiano di una decisione di adeguatezza della Commissione ([184]) e le istituzioni e gli organi dell'Unione sono attualmente considerati dall'OEB in grado di fornire un livello di protezione adeguato ([185]).

(70) Ai sensi delle DPR, in mancanza di una decisione di adeguatezza, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali a destinatari al di fuori dell'OEB solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi ([186]). Tali garanzie adeguate possono essere incluse negli accordi amministrativi con le autorità pubbliche o le organizzazioni internazionali, nelle clausole contrattuali (previa consultazione del DPB) ([187]) o nei meccanismi di certificazione ([188]). Il DPO ha elaborato una sintesi delle disposizioni da includere negli accordi amministrativi ([189]). È inoltre disponibile un modello di accordo sulla protezione dei dati per i trasferimenti ai responsabili del trattamento ([190]). Secondo gli orientamenti del DPO, l'OEB deve valutare se all'importatore di dati sarebbe impedito di adempiere agli obblighi che gli incombono in forza di uno strumento di trasferimento a causa del quadro giuridico cui è soggetto e, se necessario, di misure supplementari ([191]). Per effettuare tale valutazione, il DPO raccomanda, nella nota sulla trasmissione e il trasferimento, di tenere conto dei pertinenti orientamenti dell'EDPB e del Garante europeo della protezione dei dati ([192]).

(71) Ai sensi delle DPR, per i trasferimenti di dati verso paesi o organizzazioni che beneficiano di una decisione di adeguatezza, nonché per i trasferimenti di dati sulla base di garanzie adeguate, l'OEB deve dimostrare la necessità e la proporzionalità di ciascun trasferimento ai fini del trattamento ([193]). Inoltre, se vi è motivo di ritenere che gli interessi legittimi degli interessati possano subire pregiudizio, l'OEB, dopo aver soppesato i diversi interessi in gioco, deve

([177]) Articolo 9, paragrafo 1, DPR.
([178]) Nota sulla trasmissione e il trasferimento, pag. 11 e nota 8. Il «paese terzo» è definito dalle DPR come un paese che non è uno Stato contraente della CBE, cfr. articolo 3, primo comma, lettera u), DPR.
([179]) Articolo 9, paragrafo 2, DPR.
([180]) Cfr. articolo 1, paragrafo 2, lettera a), DPR, in combinato disposto con l'articolo 10, paragrafo 2, lettera a), CBE e con l'articolo 9, paragrafo 2, DPR.
([181]) Articolo 9, paragrafo 3, DPR.
([182]) «Outline of the EPO adequacy referential», disponibile all'indirizzo https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-adequacy-referential-methodology.pdf.
([183]) Nota 49 della nota sulla trasmissione e il trasferimento.
([184]) Ad eccezione del quadro UE-USA in materia di protezione dei dati.
([185]) Cfr. il documento «Decision of the President of the European Patent Office of 17 November 2022 concerning countries and entities considered to ensure adequate protection of personal data», disponibile all'indirizzo https://www.epo.org/en/legal/official-journal/2022/12/a111.html.
([186]) Articolo 9, paragrafi 4 e 5, DPR.
([187]) A tale riguardo, gli orientamenti del DPO fanno riferimento alle clausole contrattuali tipo adottate dalla Commissione europea, in quanto forniscono una buona panoramica delle garanzie da includere, cfr. la nota sulla trasmissione e il trasferimento, pag. 8.
([188]) Articolo 9, paragrafo 5, DPR. Cfr. anche la nota sulla trasmissione e il trasferimento, pag. 8.
([189]) «Overview of the requirements of the EPO's Administrative Arrangement models», disponibile all'indirizzo https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-epo's-administrative-arrangements-modules.pdf.
([190]) Cfr. allegato E del documento «General Conditions of Contract» dell'OEB, disponibile all'indirizzo https://link.epo.org/web/general_conditions_of_contract_en.pdf.
([191]) Nota sulla trasmissione e il trasferimento, pag. 9.
([192]) Nota sulla trasmissione e il trasferimento, pag. 9.
([193]) Articolo 9, paragrafo 6, DPR. Nel caso in cui vi sia motivo di presumere che l'interesse legittimo dell'interessato possa subire pregiudizio, il responsabile del trattamento, dopo aver soppesato i diversi interessi in gioco, deve stabilire che il trasferimento per tale finalità specifica è proporzionato.

stabilire che il trasferimento è proporzionato ([194]). Deve essere altresì garantito (attraverso garanzie contrattuali) che il destinatario possa trattare o utilizzare i dati solo per le finalità per le quali sono stati trasferiti e sia tenuto a cancellarli non appena la finalità è stata raggiunta ([195]).

(72) Ai sensi delle DPR, in assenza di una decisione di adeguatezza o di garanzie adeguate, il trasferimento di dati personali al di fuori dell'OEB è consentito «solo in via eccezionale» se si applica una cosiddetta «deroga» a condizioni analoghe a quelle previste dalle corrispondenti disposizioni del diritto dell'Unione in materia di protezione dei dati ([196]). Ciò si verifica quando a) l'interessato ha esplicitamente acconsentito al trasferimento ([197]); b) e c) il trasferimento è occasionale e necessario all'esecuzione di un contratto concluso con l'interessato o nel suo interesse (ovvero all'esecuzione di misure precontrattuali su istanza dell'interessato) ([198]); d) il trasferimento è necessario all'esecuzione di un compito nell'esercizio delle attività ufficiali dell'OEB o nell'esercizio legittimo dei poteri di cui è investito il titolare del trattamento ([199]); e) il trasferimento è occasionale e necessario per accertare, esercitare o difendere un diritto in sede giudiziaria ([200]); f) il trasferimento è necessario per tutelare un interesse vitale di una persona, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso ([201]); o g) il trasferimento avviene a partire da un registro predisposto per l'informazione del pubblico e aperto alla consultazione del pubblico o di chiunque possa dimostrare un interesse legittimo, nella misura in cui nel caso specifico siano rispettate le condizioni previste per tale consultazione ([202]). Per sua natura, e secondo gli orientamenti del DPO, tali deroghe non possono essere invocate per trasferimenti sistematici e regolari ([203]).

(73) Infine, per quanto riguarda i trasferimenti di specifiche categorie di dati a paesi o organizzazioni che non beneficiano di una decisione di adeguatezza, il Presidente può limitare ulteriormente tali trasferimenti per importanti motivi connessi all'esercizio legittimo dei pubblici poteri di cui è investito l'Ufficio ([204]). Finora il Presidente non si è avvalso di tali poteri.

2.4.8. ***Responsabilizzazione***

(74) Secondo il principio di responsabilizzazione, i soggetti che trattano dati sono tenuti a mettere in atto misure tecniche e organizzative adeguate per rispettare efficacemente i loro obblighi in materia di protezione dei dati e per essere in grado di dimostrare tale rispetto, in particolare all'autorità di controllo competente.

(75) L'articolo 4, paragrafo 1, DPR stabilisce un principio generale di responsabilizzazione, precisando che il titolare del trattamento è responsabile del rispetto delle DPR e deve essere in grado di dimostrarlo. In particolare, il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare il rispetto delle norme, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle

([194]) Articolo 9, paragrafo 6, DPR.
([195]) Articolo 9, paragrafo 6, DPR.
([196]) Cfr. l'articolo 10 DPR nonché la nota sulla trasmissione e il trasferimento, pag. 9-11.
([197]) Articolo 10, paragrafo 1, lettera a), DPR. In questo caso la persona deve essere informata dei possibili rischi dovuti all'assenza di un livello di protezione adeguato e di garanzie adeguate. Tale deroga non può essere invocata dall'OEB nell'esercizio delle sue attività ufficiali (articolo 10, paragrafo 2, DPR).
([198]) Articolo 10, paragrafo 1, lettere b) e c), e paragrafo 2, DPR. Tali deroghe non possono essere invocate dall'OEB nell'esercizio delle sue attività ufficiali (articolo 10, paragrafo 2, DPR).
([199]) Articolo 10, paragrafo 1, lettera d), DPR. Tali attività ufficiali o pubblici poteri devono essere stabiliti sulla base della CBE o di altre disposizioni giuridiche applicabili dell'Organizzazione europea dei brevetti (articolo 10, paragrafo 4, DPR). Ciò comprende il trattamento necessario per la gestione e il funzionamento dell'Ufficio o per l'adempimento degli obblighi derivanti dal dovere di cooperazione dell'OEB con gli Stati contraenti. I trasferimenti possono avvenire, ad esempio, per adempiere obblighi tra l'Ufficio e gli organismi nazionali, le amministrazioni fiscali o doganali, le autorità di controllo finanziario e i servizi competenti in materia di sicurezza sociale o di sanità pubblica, ad esempio nel caso del tracciamento dei contatti per le malattie contagiose (articolo 10, paragrafo 6, DPR).
([200]) Articolo 10, paragrafo 1, lettera e), e paragrafo 2, DPR.
([201]) Articolo 10, paragrafo 1, lettera f), DPR.
([202]) Articolo 10, paragrafo 1, lettera g), DPR. Tale trasferimento non deve riguardare la totalità dei dati personali o delle categorie di dati contenuti nel registro, salvo ove autorizzato dalle disposizioni giuridiche dell'Organizzazione europea dei brevetti; inoltre, quando il registro è destinato a essere consultato dalle persone aventi un legittimo interesse, i dati possono essere trasferiti soltanto se tali persone lo richiedono o ne sono destinatarie, tenendo pienamente conto degli interessi e dei diritti fondamentali dell'interessato (articolo 10, paragrafi 2 e 5, DPR).
([203]) Nota sulla trasmissione e il trasferimento, pag. 10.
([204]) Che, come indicato in precedenza, comprende il trattamento necessario per la sua gestione e il suo funzionamento o in virtù degli obblighi derivanti dal suo dovere di cooperazione con gli Stati contraenti. Cfr. articolo 10, paragrafo 6, DPR.

finalità del trattamento, nonché della probabilità e gravità diverse di eventuali rischi per i diritti delle persone fisiche ([205]). A tale riguardo, le DPR attuano anche i principi della tutela della vita privata fin dalla progettazione e per impostazione predefinita, imponendo al titolare del trattamento di attuare misure volte ad attuare i principi di protezione dei dati e a garantire il rispetto delle DPR, nonché a garantire che, per impostazione predefinita, siano trattati solo i dati personali necessari per ciascuna specifica finalità del trattamento ([206]).

(76) Il titolare del trattamento e i responsabili del trattamento devono tenere un registro delle attività di trattamento contenente, tra l'altro, informazioni sulla finalità del trattamento, sulle categorie di dati trattati, sulle categorie di destinatari cui sono comunicati i dati e su eventuali trasferimenti di dati personali ([207]). Tali registrazioni sono, in linea di principio, accessibili al pubblico (a meno che non contengano informazioni riservate) e incluse in un registro per la protezione dei dati accessibile al pubblico e devono essere messe a disposizione del DPB su richiesta ([208]). Ciascuna unità operativa deve inoltre nominare almeno una persona di collegamento per la protezione dei dati (con un mandato rinnovabile da uno a tre anni), che deve seguire una formazione obbligatoria in materia di protezione dei dati e assistere il titolare del trattamento nell'adempimento dei propri obblighi ([209]).

(77) Infine le DPR forniscono diversi strumenti che possono assistere il titolare del trattamento e i responsabili del trattamento nei loro sforzi di conformità. Ad esempio, ai sensi delle DPR, l'adesione a meccanismi di certificazione approvati può fungere da prova del rispetto degli obblighi delle DPR ([210]). Inoltre, a determinate condizioni, le DPR richiedono lo svolgimento di una valutazione d'impatto sulla protezione dei dati o una consultazione preliminare del DPO e del DPB. Una valutazione d'impatto sulla protezione dei dati è richiesta quando un tipo di trattamento può comportare un rischio elevato per i diritti e le libertà di una persona ([211]). Ciò si verifica, ad esempio, nel caso di una valutazione sistematica e approfondita degli aspetti personali su cui si basano le decisioni automatizzate o nel caso di un trattamento su larga scala di categorie particolari di dati ([212]). Se una valutazione d'impatto indica che il trattamento comporterebbe un rischio elevato per i diritti e le libertà delle persone e che il rischio non può essere attenuato da misure di sicurezza ragionevoli, il titolare del trattamento deve consultare il DPB ([213]). Il DPB deve fornire un parere scritto se ritiene che il trattamento previsto violi le DPR ([214]). Più in generale, il titolare del trattamento è tenuto a consultare il DPO quando elabora norme o documenti operativi sull'attuazione delle limitazioni ai diritti individuali ([215]).

2.5. **Controllo e applicazione delle norme**

(78) Al fine di garantire un livello di protezione adeguato dei dati nella pratica, dovrebbe esistere un'autorità di controllo indipendente cui siano conferiti i poteri di monitorare e assicurare il rispetto delle norme in materia di protezione dei dati. Tale autorità dovrebbe agire in piena indipendenza e imparzialità nell'esercizio delle sue funzioni e dei suoi poteri.

(79) Il quadro giuridico dell'OEB affida a due organismi il controllo del rispetto delle norme in materia di protezione dei dati da parte dell'Organizzazione: il DPO e il DPB. Entrambi gli organismi sono istituiti dall'articolo 32 bis dello statuto, mentre il loro status e i loro poteri sono ulteriormente specificati nelle DPR ([216]). I loro ruoli sono complementari e implicano la cooperazione, ma ogni organismo rimane indipendente nelle proprie funzioni.

([205]) Articolo 26, paragrafo 1, DPR.
([206]) Articolo 27, paragrafi 1 e 2, DPR.
([207]) Articolo 32, paragrafi 1 e 2, DPR. A norma dell'articolo 4, paragrafo 1, DPR, il titolare del trattamento deve seguire «un approccio strutturato e basato sul rischio per progettare e documentare le operazioni di trattamento». Il titolare del trattamento deve inoltre essere in grado di dimostrare agli interessati in qualsiasi momento che gli impegni e le condizioni documentati sono rispettati durante le operazioni di trattamento.
([208]) Articolo 32, paragrafi 4, 5 e 6, DPR.
([209]) Articolo 45 DPR.
([210]) Articolo 26, paragrafo 3, DPR.
([211]) Il titolare del trattamento deve chiedere il parere del DPO sulla necessità di effettuare una valutazione d'impatto, e il DPO può a sua volta può consultare il DPB in caso di dubbio. Cfr. anche l'articolo 38, paragrafi 1 e 2, DPR.
([212]) Articolo 38, paragrafo 4, DPR.
([213]) Articolo 38, paragrafo 6, DPR.
([214]) Articolo 38, paragrafi 7 e 8, e articolo 39 DPR.
([215]) Articolo 40, paragrafo 2, DPR.
([216]) Articolo 32 bis, paragrafi 1 e 2, dello statuto, che attribuisce al DPO il ruolo di monitorare l'applicazione delle disposizioni in materia di protezione dei dati personali, consigliare le varie unità operative dell'OEB in merito all'adempimento dei loro obblighi e fornire loro la documentazione operativa necessaria per l'attuazione pratica delle prescrizioni in materia di protezione dei dati. Il DPB è tenuto a garantire un «controllo indipendente, efficace e imparziale delle disposizioni applicabili alla protezione dei dati personali». Può esistere un diverso meccanismo di controllo indipendente finalizzato ad assicurare il rispetto delle norme da parte delle commissioni di ricorso quando trattano dati personali nell'esercizio delle loro funzioni giurisdizionali (cfr. anche l'articolo 2, paragrafo 6, DPR).

2.5.1. ***Indipendenza***

(80) Ai sensi dello statuto, il DPO e il DPB agiscono in piena indipendenza da qualsiasi interferenza interna o esterna nello svolgimento dei loro compiti e nell'esercizio dei loro poteri ([217]). Tale principio è integrato da diverse garanzie supplementari che assicurano la loro indipendenza.

(81) Il DPO (e i suoi vice) sono nominati dal Presidente sulla base delle loro qualifiche professionali e, in particolare, della loro conoscenza specialistica della legislazione e delle prassi in materia di protezione dei dati ([218]). Il DPO è nominato per un mandato rinnovabile da tre a cinque anni. Il DPB è consultato prima di qualsiasi proposta di destituzione o rimozione del DPO dal suo ruolo ([219]). Tale consultazione preliminare prima della destituzione o della rimozione del DPO è intesa a garantire un ulteriore controllo e riesame in caso di proposta di destituzione o di rimozione. La destituzione o rimozione può essere proposta per uno dei motivi seguenti ([220]): se il DPO non soddisfa più le condizioni richieste per l'esercizio delle funzioni ([221]); per insufficienza professionale ([222]); o a seguito di provvedimenti disciplinari ([223]). Le DPR stabiliscono inoltre che il DPO non può essere destituito o sanzionato per aver svolto i suoi compiti e non può ricevere istruzioni ([224]). Il DPO deve essere coinvolto in tutte le questioni relative alla protezione dei dati personali e presenta relazioni annuali di attività al Presidente e al Consiglio d'amministrazione ([225]). L'Ufficio deve fornire al DPO le risorse necessarie per lo svolgimento dei suoi compiti ([226]).

(82) Il DPB è composto da tre esperti esterni nel settore della protezione dei dati, vale a dire un presidente e altri due membri ([227]), nonché un supplente, nominati dal Presidente dell'OEB per un mandato rinnovabile di tre anni ([228]). I membri del DPB devono possedere le qualifiche richieste per l'esercizio di funzioni giurisdizionali o essere professionisti della protezione dei dati con competenze ed esperienza comprovate nel settore del diritto in materia di protezione dei dati acquisite a livello nazionale o internazionale. Non possono essere dipendenti dell'OEB o essere stati impiegati presso quest'ultima negli ultimi dieci anni ([229]). Ai sensi dell'articolo 48, paragrafo 6, DPR, i membri del DPB sono completamente indipendenti nell'esercizio delle loro funzioni. In particolare, non possono chiedere istruzioni all'Ufficio o al Consiglio d'amministrazione e non possono essere vincolati da tali istruzioni. Il regolamento interno del DPB prevede altresì che il DPB debba agire in modo imparziale e in piena indipendenza

([217]) Articolo 32 bis, paragrafi 4 e 5, dello statuto.
([218]) Articolo 41 DPR.
([219]) Articolo 42, paragrafo 8, DPR. Tale consultazione ha luogo a prescindere dal motivo o dalla ragione invocati per la proposta di destituzione o rimozione.
([220]) Articolo 50 dello statuto.
([221]) Cfr. l'articolo 53, paragrafo 1, dello statuto, ai sensi del quale «l'autorità che ha il potere di nomina può decidere di porre fine al servizio di un lavoratore: a) se lo Stato contraente di cui il lavoratore è cittadino cessa di essere parte della convenzione; b) se il lavoratore rifiuta di essere trasferito in un paese diverso da quello in cui presta servizio; c) se, nel caso di un lavoratore nominato dal Consiglio d'amministrazione a norma dell'articolo 11, paragrafi 1 e 2, della convenzione, il Consiglio d'amministrazione decide in tal senso nell'interesse dell'Organizzazione; d) che è in servizio ininterrottamente da un anno o meno in virtù di una nomina a tempo determinato; e) se, a seguito delle proprie azioni, il lavoratore cessa di soddisfare le condizioni di cui all'articolo 8, lettera a) o b) (vale a dire essere cittadino di uno degli Stati contraenti dell'OEB, salvo deroga autorizzata dall'autorità che ha il potere di nomina, e godere di pieni diritti civili e politici); o f) negli altri casi espressamente previsti dallo statuto».
Cfr. anche l'articolo 13, paragrafo 4, lettera b), dello statuto, ai sensi del quale «un rapporto sul funzionario in prova può essere redatto in qualsiasi momento durante il periodo di prova, qualora l'esercizio delle sue funzioni, il suo rendimento e il suo comportamento si rivelino insufficienti. Sulla base del rapporto o dei rapporti sul periodo di prova, l'autorità che ha il potere di nomina può:
- licenziare una persona neoassunta in prova,
- decidere che il funzionario in prova trasferito, promosso o riassegnato ritorni al suo posto precedente o, se questo è stato occupato, a un impiego corrispondente al grado del suo impiego precedente per il quale soddisfa i requisiti».
([222]) L'articolo 52 dello statuto stabilisce i criteri e le procedure da seguire qualora sia constatata un'«insufficienza professionale».
([223]) Articolo 94 dello statuto.
([224]) Articolo 42, paragrafo 3, DPR. Sebbene il DPO possa svolgere anche altri compiti, tali compiti non possono dar luogo a un conflitto di interessi (articolo 42, paragrafo 6, DPR).
([225]) Articolo 42, paragrafi 1 e 3, DPR.
([226]) Articolo 42, paragrafo 2, DPR.
([227]) Articolo 48, paragrafo 1, DPR.
([228]) Articolo 48, paragrafi 1 e 3, DPR.
([229]) Articolo 48, paragrafo 2, DPR.

nello svolgimento dei suoi compiti ([230]). Inoltre l'OEB può destituire i membri del DPB solo per gravi motivi ([231]). I membri del DPB sono vincolati da un obbligo di riservatezza ([232]) e devono astenersi dall'agire nel caso in cui abbiano un conflitto di interessi, in particolare un interesse personale ([233]). L'OEB è tenuta a sostenere il DPB nello svolgimento dei suoi compiti fornendo a quest'ultimo le risorse necessarie, nonché sostegno giuridico e amministrativo (tramite una segreteria e accordando al DPB l'accesso ai dati personali e alle operazioni di trattamento) ([234]).

2.5.2. ***Compiti e poteri***

(83) I compiti del DPO comprendono quanto segue: informare il titolare del trattamento o i responsabili del trattamento dei loro obblighi e consigliarli di conseguenza; sensibilizzare e formare il personale coinvolto nelle operazioni di trattamento; garantire che gli interessati siano informati dei propri diritti ai sensi delle DPR; e monitorare in modo indipendente l'applicazione interna e il rispetto delle DPR, nonché di altre disposizioni giuridiche dell'OEB aventi implicazioni in materia di protezione dei dati ([235]). Gli interessati possono contattare il DPO per qualsiasi questione relativa al trattamento dei loro dati o all'esercizio dei loro diritti ([236]), e il titolare del trattamento e i responsabili del trattamento possono consultare il DPO su qualsiasi questione relativa all'interpretazione e all'applicazione delle DPR ([237]).

(84) Nell'ambito del suo ruolo di controllo, il DPO ha il potere di effettuare audit e indagini sulla protezione dei dati ([238]). Gli audit sono avviati dal DPO conformemente a un piano di audit annuale preparato in consultazione con il DPB ([239]). Un audit si concentra sulla valutazione delle registrazioni, delle dichiarazioni e della documentazione pertinente in materia di protezione dei dati, ad esempio per verificare l'esattezza e la completezza della documentazione, la corretta applicazione delle metodologie di gestione dei rischi, l'esattezza e la tempestività delle risposte agli interessati o il corretto svolgimento delle valutazioni d'impatto sulla protezione dei dati e il loro numero ([240]). Secondo le informazioni trasmesse alla Commissione dal DPO, sono stati effettuati tre audit nel 2023 e quattro nel 2024. Un'indagine può essere avviata dal DPO di propria iniziativa, sulla base di una richiesta ricevuta dal DPB o da un organismo all'interno dell'OEB (ad esempio il Presidente o un titolare del trattamento delegato) o sulla base di informazioni ricevute in altro modo (anche, ad esempio, da terzi e persone fisiche) ([241]). Le indagini richieste dal DPB sono condotte dal DPO in maniera indipendente. Il DPB può formulare osservazioni e/o richiedere un'indagine supplementare su eventuali questioni che potrebbero emergere ([242]). Le ispezioni si concentrano sulle operazioni di trattamento o su aspetti particolari delle stesse o su eventi ad esse connessi, al fine di garantire che il trattamento in questione soddisfi le prescrizioni delle DPR e di garantire la tutela dei diritti e delle libertà degli interessati ([243]).

(85) Il DPO ha accesso a tutte le informazioni pertinenti, compresi i dati personali trattati, nonché a tutti gli uffici, alle installazioni per il trattamento dei dati e ai supporti di dati ([244]). Tutti i dipendenti e le unità operative dell'OEB sono tenuti ad assistere il DPO nell'esercizio delle sue funzioni, anche fornendo accesso ai locali e alle informazioni pertinenti ([245]).

([230]) Articolo 1, paragrafo 1, del regolamento interno del comitato per la protezione dei dati, CA/26/21 Add. 1, adottato l'11 giugno 2021. Disponibile all'indirizzo https://link.epo.org/web/data_protection_board-rules_of_procedure_en.pdf.

([231]) In particolare, l'accordo sulle prestazioni prevede che «il mandato può essere risolto (dal membro del DPB) (solo) con un preavviso scritto di sei (6) mesi, fatto salvo il diritto di risoluzione per gravi motivi». Poiché l'accordo è disciplinato dal diritto tedesco, la nozione di grave motivo deve essere interpretata conformemente all'articolo 626 del codice civile tedesco. Secondo la giurisprudenza, un grave motivo può sussistere ad esempio in caso di violazione ripetuta e persistente degli obblighi applicabili (ad esempio per quanto riguarda il conflitto di interessi) o in caso di detenzione.

([232]) Articolo 48, paragrafo 5, DPR.

([233]) Articolo 48, paragrafo 7, DPR.

([234]) Articolo 48, paragrafo 10, DPR. La segreteria svolge i suoi compiti indipendentemente da qualsiasi indebita interferenza ed esclusivamente su istruzioni del Presidente del DPB. Essa presta assistenza in materia di analisi, amministrativa e logistica al comitato. Cfr. l'articolo 2 del regolamento interno del DPB.

([235]) Articolo 43, paragrafo 1, DPR.

([236]) Articolo 43, paragrafo 1, lettera k), DPR.

([237]) Articolo 42, paragrafi 4 e 7, DPR.

([238]) Articolo 43, paragrafo 1, lettera d), DPR. Cfr. anche la nota sul controllo in materia di protezione dei dati «How the Data Protection Office Conducts DP Audits and DP Inspections», disponibile all'indirizzo https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-data-protection-oversight-mechanism.pdf.

([239]) Il DPB può formulare suggerimenti sui settori in cui dovrebbero essere effettuati audit, cfr. la nota sul controllo in materia di protezione dei dati, pag. 4.

([240]) Nota sul controllo in materia di protezione dei dati, pag. 4.

([241]) Nota sul controllo in materia di protezione dei dati, pag. 7.

([242]) Nota sul controllo in materia di protezione dei dati, pag. 6.

([243]) Nota sul controllo in materia di protezione dei dati, pag. 6.

([244]) Articolo 43, paragrafo 5, DPR.

([245]) Articolo 46 DPR.

(86) Alla conclusione di un audit o di un'indagine, il DPO adotta una relazione in cui espone le risultanze, le conclusioni e le misure correttive raccomandate ([246]). Tali misure possono comprendere, ad esempio, misure preventive o di attenuazione volte a migliorare il rispetto delle norme, nonché misure per porre rimedio alla non conformità (ad esempio per rendere il trattamento conforme alle DPR, trattare le richieste degli interessati di esercitare i loro diritti, sospendere o cessare un trattamento ecc.) ([247]). Il DPO può inoltre portare all'attenzione dell'autorità competente che ha il potere di nomina le violazioni delle DPR da parte dei dipendenti e raccomandare l'avvio di un'indagine amministrativa per stabilire se sia necessario un intervento disciplinare o di altro tipo ([248]). Qualsiasi dipendente che non rispetti le DPR, intenzionalmente o per negligenza, è passibile di sanzioni disciplinari o di altre azioni ai sensi dello statuto ([249]).

(87) L'esito degli audit e delle indagini deve essere comunicato al DPB ([250]). La relazione di audit o d'indagine deve essere condivisa con il DPB su richiesta. Il DPB è autorizzato a presentare osservazioni sulla relazione del DPO, anche per quanto riguarda le risultanze del DPO in merito all'esistenza o meno di una violazione delle DPR e le misure correttive proposte, e può chiedere ulteriori atti d'indagine ([251]). Se un audit o un'ispezione del DPO porta a concludere che vi è stata una non conformità (vale a dire una violazione delle DPR), la relazione del DPO deve essere trasmessa al DPB per convalida delle conclusioni e delle misure correttive raccomandate. Qualora non concordi con le conclusioni o le misure correttive raccomandate dal DPO, il DPB gli comunica le proprie osservazioni, anche per modificare le conclusioni proposte e le misure correttive raccomandate, e il DPO dovrebbe attuarle di conseguenza. Le misure correttive convalidate dal DPB sono vincolanti per il titolare del trattamento e i titolari del trattamento delegati e possono essere invocate dalle persone fisiche prima dei meccanismi di ricorso di cui al considerando 95 ([252]). Il DPO deve verificare l'attuazione delle misure correttive (in linea di principio sei mesi dopo la loro comunicazione) e riferire annualmente al Presidente in merito allo stato di attuazione ([253]).

(88) Oltre al ruolo di garantire il rispetto delle DPR, altri compiti del DPB comprendono la consulenza al Presidente in merito all'adozione di decisioni di adeguatezza, la consulenza al titolare del trattamento sulla necessità di effettuare una valutazione d'impatto sulla protezione dei dati e l'esame dei reclami delle persone fisiche (cfr. considerando da 92 a 96) ([254]).

2.6. **Mezzi di ricorso**

(89) Al fine di garantire una protezione adeguata e, in particolare, il rispetto dei diritti individuali, l'interessato dovrebbe avere a disposizione mezzi di ricorso efficaci, compreso il risarcimento dei danni.

(90) Il quadro giuridico dell'OEB offre mezzi di ricorso alle persone fisiche attraverso una combinazione di diverse vie.

(91) In primo luogo, gli interessati che ritengono che il trattamento dei loro dati personali da parte dell'OEB violi i loro diritti (ossia violi le DPR) possono presentare una domanda di riesame da parte del titolare del trattamento delegato conformemente all'articolo 49 DPR. Il titolare del trattamento delegato riesamina il reclamo e adotta una decisione ([255]). Prima di adottare una decisione, il titolare del trattamento delegato deve consultare il DPO, il quale fornisce un parere scritto entro quindici giorni di calendario dal ricevimento della domanda di riesame ([256]). Il titolare

([246]) Nota sul controllo in materia di protezione dei dati.
([247]) Nota sul controllo in materia di protezione dei dati, pag. 2(definizione di «raccomandazioni»).
([248]) Articolo 43, paragrafo 6, DPR.
([249]) Articolo 54 DPR. Le sanzioni disciplinari sono imposte dal Presidente, il quale esercita l'autorità disciplinare e dispone di poteri disciplinari nei confronti del personale dell'OEB, cfr. articolo 10 CBE e articolo 93 e segg. dello statuto.
([250]) Nota sul controllo in materia di protezione dei dati, pag. 7.
([251]) Nota sul controllo in materia di protezione dei dati, pag. 3, 4 e 8.
([252]) «Decision of the President of the European Patent Office dated 12.07.2024 on the Enforceability of DPO Recommendations endorsed by the Data Protection Board in the framework of Data Protection Audits and Inspections», 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 sul controllo in materia di protezione dei dati, pag. 5 e 9.
([254]) Articolo 47 DPR.
([255]) Articolo 49, paragrafo 1, DPR. La domanda deve essere presentata entro tre mesi dal giorno in cui l'interessato è stato informato o è altrimenti venuto a conoscenza del trattamento di dati personali che presumibilmente viola i suoi diritti.
([256]) Articolo 49, paragrafo 2, DPR. Se il DPO non fornisce un parere entro la fine di tale periodo, il parere non è più necessario.

del trattamento delegato deve rispondere alla persona fisica entro un mese dalla data di ricevimento della richiesta ([257]). La decisione deve essere comunicata alla persona fisica, unitamente a informazioni sulla possibilità di un ulteriore ricorso ([258]). Se il titolare del trattamento delegato non intraprende alcuna azione entro tre mesi, si considera che la richiesta sia implicitamente rigettata.

(92) In secondo luogo, le persone fisiche possono contestare una decisione o il rigetto implicito di una domanda di riesame da parte del titolare del trattamento delegato presentando un reclamo al DPB ([259]).

(93) Nell'esaminare un reclamo, il DPB deve invitare l'interessato, il titolare del trattamento e, se del caso, il responsabile del trattamento a esporre per iscritto la propria posizione sulle asserzioni e sui fatti in questione e a fornire prove o osservazioni e argomentazioni sulle prove disponibili ([260]). In tale contesto, il DPB può chiedere alle parti tutte le informazioni di cui ha bisogno per trattare il reclamo e può inoltre ottenere ulteriori informazioni tramite il DPO ([261]). Nel decidere sul seguito da dare a un reclamo, il DPB deve tener conto, tra l'altro, della natura e della gravità della presunta violazione, del numero di interessati coinvolti, delle categorie di dati interessate e della durata della violazione ([262]). Il DPB può invitare le parti a cercare una composizione amichevole e incoraggia e facilita attivamente una tale composizione ([263]). Il reclamante può inoltre chiedere al DPB di applicare una procedura d'urgenza per motivi di gravità della presunta violazione o a causa della gravità del rischio imposto ai diritti delle persone fisiche ([264]).

(94) Dopo aver esaminato un reclamo, il DPB invia un parere motivato al titolare del trattamento, che include un'esposizione dei fatti, le principali argomentazioni delle parti, le considerazioni del DPB e le sue raccomandazioni ([265]). In caso di procedura d'urgenza, il DPB deve formalmente emettere un parere motivato entro due mesi dalla presentazione del reclamo ([266]). Nel parere motivato il DPB può formulare tutte le raccomandazioni che ritiene necessarie, tra cui provvedimenti ingiuntivi (ad esempio per la cessazione del trattamento illecito dei dati o la cancellazione di dati trattati illecitamente) e risarcimento dei danni materiali o immateriali ([267]). Il parere motivato deve essere comunicato all'interessato e al titolare del trattamento (ossia al Presidente dell'Ufficio, al Presidente delle commissioni di ricorso, al Presidente del Consiglio d'amministrazione o al Presidente del Comitato ristretto, a seconda che il reclamo riguardi l'Ufficio, le commissioni di ricorso, il Consiglio o il Comitato ristretto). Il titolare del trattamento prende poi una decisione vincolante definitiva, facendo seguito al parere motivato del DPB ([268]). La decisione definitiva è comunicata all'interessato, al DPB e al DPO ([269]). Se decide di non seguire uno o più aspetti del parere motivato, il titolare del trattamento ne spiega per iscritto i motivi nella decisione ([270]).

(95) L'interessato che non sia soddisfatto della decisione del titolare del trattamento può impugnarla ulteriormente, facendo riferimento, nell'atto di impugnazione, al parere motivato del DPB. I dipendenti dell'OEB possono impugnare la decisione dinanzi al tribunale amministrativo dell'Organizzazione internazionale del lavoro ([271]). Qualsiasi altro interessato che non sia d'accordo con la decisione del titolare del trattamento può presentare al Presidente una domanda di arbitrato ad hoc entro tre mesi dal ricevimento della decisione ([272]). Le DPR prevedono

([257]) Articolo 49, paragrafo 3, DPR. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. In caso di proroga, il titolare del trattamento delegato deve darne notifica all'interessato entro un mese dal ricevimento della domanda di riesame, indicando i motivi del ritardo.

([258]) Articolo 49, paragrafo 3, DPR.

([259]) Articolo 50, paragrafo 1, DPR. Un reclamo dinanzi al DPB deve essere presentato entro tre mesi dal ricevimento della decisione o, in caso di rigetto implicito, dalla data di scadenza del termine per rispondere alla domanda.

([260]) Articolo 50, paragrafo 2, DPR.

([261]) In particolare, il DPO ha l'obbligo di rispondere alle richieste del DPB e di cooperare con esso (articolo 43, lettera i), DPR). Il DPO è inoltre tenuto ad agevolare la cooperazione tra il DPB e l'Ufficio e in tale contesto ha accesso a qualsiasi informazione pertinente (articolo 43, lettera j), articolo 46, lettere a) e b), DPR).

([262]) Articolo 4, paragrafo 5, del regolamento interno del DPB.

([263]) Articolo 8 del regolamento interno del DPB.

([264]) Articolo 11, paragrafo 1, del regolamento interno del DPB.

([265]) Articolo 10, paragrafo 2, del regolamento interno del DPB.

([266]) Articolo 11, paragrafo 2, del regolamento interno del DPB.

([267]) Articolo 50, paragrafo 3, DPR.

([268]) Articolo 50, paragrafo 4, DPR e articolo 10, paragrafo 6, del regolamento interno del DPB.

([269]) Articolo 50, paragrafo 6, DPR.

([270]) Articolo 50, paragrafo 4, DPR. Se le raccomandazioni del DPB non sono direttamente pertinenti per gli interessati, l'eventuale scostamento è indicato per iscritto dal titolare del trattamento tramite un documento presentato al DPB.

([271]) Articolo 50, paragrafo 7, DPR. Cfr. l'articolo 13 CBE e l'articolo 113 dello statuto.

([272]) Articolo 50, paragrafo 8, e articolo 52, paragrafo 2, DPR. Ai sensi delle AC DPR e delle SC DPR, l'arbitrato può essere richiesto al Presidente del Consiglio d'amministrazione.

una procedura specifica da seguire in caso di arbitrato ad hoc ([273]). In particolare, entro tre mesi dal ricevimento della domanda dell'interessato, il Segretario generale della Corte permanente di arbitrato deve nominare un arbitro sulla base dei criteri stabiliti nelle DPR ([274]). L'arbitro deve avere una formazione di giurista, essere abilitato a esercitare la professione forense in uno degli Stati contraenti dell'OEB, essere in grado di dimostrare competenze pertinenti in materia di protezione dei dati e conoscere il diritto che disciplina le organizzazioni internazionali ([275]). Oltre a soddisfare tali criteri, possono essere nominate solo persone che non hanno lavorato per l'OEB o per l'interessato o al loro servizio. Le DPR prevedono che l'arbitro debba agire in modo indipendente e imparziale ([276]), trattare ciascuna parte su un piano di parità e dare alle parti la possibilità di far valere le rispettive ragioni in ogni fase del procedimento ([277]). I procedimenti arbitrali non sono pubblici ([278]) e sono disciplinati dalla CBE, dalle DPR, compresa qualsiasi normativa di attuazione, dal diritto delle organizzazioni internazionali e dai principi del diritto internazionale pubblico ([279]). Ciascuna parte deve sostenere i propri costi e le proprie spese di rappresentanza legale (salvo decisione contraria dell'arbitro), mentre gli onorari e le spese dell'arbitro, nonché le spese per eventuali pareri di esperti e testimoni sono a carico dell'OEB ([280]). La transazione deve essere conclusa sotto forma di lodo arbitrale scritto con una formulazione concordata, definitiva e vincolante ([281]).

(96) Chiunque abbia subito un danno a seguito di una violazione delle DPR può chiedere un risarcimento all'OEB utilizzando le procedure descritte ai considerando da 91 a 95 ([282]). L'OEB non sarà ritenuta responsabile se dimostra di non essere all'origine dell'evento che ha causato il danno.

3. ACCESSO AI DATI PERSONALI TRASFERITI DALL'UNIONE ALL'UFFICIO EUROPEO DEI BREVETTI E LORO UTILIZZO DA PARTE DELLE AUTORITÀ PUBBLICHE

(97) Il quadro giuridico nell'ambito del quale l'OEB valuta le richieste delle autorità pubbliche, nei suoi Stati contraenti e nei paesi terzi, in merito ai dati personali trattati dall'OEB e risponde ad esse deriva dal documento dell'OEB «Protocol on Privileges and Immunities» (PPI) ([283]), dalle prescrizioni delle DPR in materia di trasmissione e trasferimento di dati personali e dal diritto internazionale pubblico.

(98) In primo luogo, il trattamento dei dati personali da parte dell'OEB ai fini delle sue attività ufficiali è coperto dalle immunità dell'Organizzazione. Le immunità dell'OEB sono integrate dal dovere di cooperazione di cui all'articolo 20 PPI. Di conseguenza, qualsiasi richiesta di un'autorità pubblica di uno Stato contraente di ottenere dati trattati dall'OEB deve essere valutata dal Presidente in conformità del PPI (articolo 20, paragrafo 1), il quale stabilisce che l'Organizzazione «coopera in qualsiasi momento con le autorità competenti degli Stati contraenti al fine di agevolare la corretta amministrazione della giustizia, garantire il rispetto dei regolamenti di polizia, dei regolamenti in materia di sanità pubblica e ispezione del lavoro o di altre normative nazionali analoghe, e prevenire qualsiasi abuso dei privilegi, delle immunità e delle agevolazioni previsti dal presente protocollo». In via eccezionale, l'Organizzazione può rinunciare alla propria immunità di giurisdizione ed esecuzione ([284]). Nel decidere in merito a una richiesta di cooperazione, il Presidente esercita un potere discrezionale e valuta se la richiesta rispetta il quadro giuridico dell'Organizzazione ([285]). La conclusione può essere che l'Ufficio può rispondere a una richiesta ai sensi del PPI ed è autorizzato a divulgare dati personali solo nel rispetto delle prescrizioni in materia di trasmissione dei dati previste dalle DPR (cfr. considerando da 62 a 67). Ai sensi delle DPR, il destinatario deve dimostrare la necessità che i dati siano trasmessi per una finalità specifica derivante dagli obblighi di cooperazione dell'OEB con lo Stato o gli Stati

([273]) Articolo 52, paragrafo 1, DPR.
([274]) Articolo 52, paragrafo 4, DPR.
([275]) Articolo 52, paragrafo 4, DPR.
([276]) Articolo 52, paragrafo 4, DPR.
([277]) Articolo 52, paragrafo 8, DPR.
([278]) Articolo 52, paragrafo 9, DPR.
([279]) Articolo 52, paragrafo 6, DPR. Il luogo dell'arbitrato è L'Aia (articolo 52, paragrafo 5, DPR) e l'arbitro deve scegliere la lingua utilizzata durante il procedimento, che deve tuttavia essere una delle lingue ufficiali dell'OEB (inglese, francese o tedesco) (articolo 52, paragrafo 7, DPR).
([280]) Articolo 52, paragrafo 13, DPR.
([281]) Articolo 52, paragrafo 10, DPR. Cfr. anche l'articolo 3 e l'articolo 34, paragrafo 2, del regolamento della Corte permanente di arbitrato.
([282]) Articolo 53 DPR. Ai sensi dell'articolo 9, paragrafo 2, CBE, a determinate condizioni (in particolare i requisiti applicabili ai sensi del diritto tedesco) i singoli possono anche ottenere il risarcimento dei danni causati dal personale dell'OEB nell'esercizio delle sue funzioni.
([283]) «Protocol on Privileges and Immunities» dell'OEB, disponibile all'indirizzo https://www.epo.org/en/legal/epc/2020/proprim.html.
([284]) Articolo 3, paragrafo 1, lettera a), PPI.
([285]) Ciò comprende la possibilità di respingere una richiesta.

contraenti ([286]). Per ciascuna trasmissione, il titolare del trattamento deve essere in grado di dimostrare che la trasmissione è necessaria e proporzionata alla finalità specifica per la quale è effettuata ([287]). Qualsiasi trasmissione di dati deve essere effettuata in un modo tale da assicurare che il livello di protezione riconosciuto dalle DPR sia mantenuto ([288]). Secondo gli orientamenti emanati dal DPO, ciò significa che devono essere predisposte garanzie adeguate, anche assicurando che i dati da condividere siano ridotti al minimo e limitati a quanto adeguato, pertinente e strettamente necessario per conseguire tale finalità ([289]). Se vi è motivo di presumere che i diritti e le libertà della persona interessata possano essere lesi, il titolare del trattamento deve dimostrare che è proporzionato trasmettere i dati personali per tale finalità specifica, dopo aver ponderato i diversi interessi in gioco ([290]).

(99) In secondo luogo, non esiste uno strumento giuridico applicabile all'OEB che disciplini specificamente il trattamento delle richieste delle autorità pubbliche di paesi terzi (vale a dire che non sono parti contraenti dell'OEB) di ottenere dati trattati dalla stessa. Di conseguenza, qualsiasi divulgazione in risposta a una tale richiesta può aver luogo solo se sono soddisfatte le prescrizioni per i trasferimenti internazionali di dati ai sensi delle DPR (come descritto ai considerando da 68 a 73). Ciò avverrebbe solo se per il paese interessato è stata adottata una decisione di adeguatezza che copra il trasferimento, se esistono garanzie adeguate o se si applica una deroga.

(100) Il rispetto del PPI da parte del Presidente, compreso il modo in cui sono state trattate le richieste di cooperazione da parte delle autorità pubbliche, è soggetto al controllo del Consiglio d'amministrazione, mentre il rispetto delle prescrizioni in materia di trasmissione e trasferimento di dati personali nelle DPR è soggetto al controllo del DPO e del DPB, come descritto ai considerando da 84 a 88. Le persone fisiche possono avvalersi delle vie di ricorso descritte nei considerando da 90 a 96 per quanto riguarda le trasmissioni o i trasferimenti dei loro dati personali in violazione delle DPR.

4. CONCLUSIONI

(101) La Commissione ritiene che l'OEB garantisca un livello di protezione dei dati personali trasferiti dall'Unione sostanzialmente equivalente a quello garantito dal regolamento (UE) 2016/679.

(102) Sulla base delle risultanze della presente decisione, è opportuno decidere che l'OEB garantisce un livello di protezione adeguato ai sensi dell'articolo 45 del regolamento (UE) 2016/679, interpretato alla luce della Carta dei diritti fondamentali dell'Unione europea, per i dati personali trasferiti dall'Unione all'OEB.

5. EFFETTI DELLA PRESENTE DECISIONE E AZIONE DELLE AUTORITÀ DI PROTEZIONE DEI DATI

(103) Gli Stati membri e i loro organi sono tenuti ad adottare le misure necessarie per conformarsi agli atti delle istituzioni dell'Unione, che si presumono legittimi e producono pertanto effetti giuridici finché non siano stati revocati o annullati nel contesto di un ricorso per annullamento ovvero dichiarati invalidi a seguito di un rinvio pregiudiziale o di un'eccezione di illegittimità.

(104) Di conseguenza, una decisione di adeguatezza adottata dalla Commissione a norma dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 è vincolante per tutti gli organi degli Stati membri che ne sono i destinatari, comprese le autorità di controllo indipendenti. In particolare i trasferimenti da un titolare del trattamento o un responsabile del trattamento nell'Unione verso l'OEB possono avvenire senza la necessità di ottenere ulteriori autorizzazioni.

([286]) Articolo 8, paragrafo 3, DPR.
([287]) Articolo 8, paragrafo 4, DPR.
([288]) Nota esplicativa «EPO transmission and transfer of personal data» (nota sulla trasmissione e il trasferimento), disponibile all'indirizzo https://link.epo.org/web/office/data-protection-and-privacy/en-explanatory-note-on-epo-transmission-and-transfer-of-personal-data.pdf, pag. 4. Si veda in particolare la frase «The EPO DPR […] lay down the general principle of adequate protection, especially applicable to international data stream» («Le DPR dell'OEB [...] stabiliscono il principio generale della protezione adeguata, applicabile soprattutto ai flussi internazionali di dati»).
([289]) Nota sulla trasmissione e trasferimento, nota 12.
([290]) Articolo 8, paragrafo 3, DPR.

(105) È opportuno ricordare che, ai sensi dell'articolo 58, paragrafo 5, del regolamento (UE) 2016/679, e come spiegato dalla Corte di giustizia nella causa C-362/14 ([291]), quando un'autorità nazionale di protezione dei dati mette in dubbio, anche in seguito a un reclamo, la compatibilità di una decisione di adeguatezza della Commissione con i diritti fondamentali della persona fisica concernenti la tutela della vita privata e la protezione dei dati, il diritto nazionale deve prevedere mezzi di ricorso che consentano di far valere tali obiezioni dinanzi a un organo giurisdizionale nazionale, che può essere tenuto a effettuare un rinvio pregiudiziale alla Corte di giustizia.

6. MONITORAGGIO, SOSPENSIONE, ABROGAZIONE O MODIFICA DELLA PRESENTE DECISIONE

(106) Secondo la giurisprudenza della Corte di giustizia, e ai sensi dell'articolo 45, paragrafo 4, del regolamento (UE) 2016/679, la Commissione dovrebbe monitorare costantemente gli sviluppi nel paese terzo o nell'organizzazione internazionale registrati dopo l'adozione di una decisione di adeguatezza, al fine di valutare se tale paese terzo o organizzazione continui a garantire un livello di protezione sostanzialmente equivalente. Tale verifica è in ogni caso obbligatoria quando la Commissione riceve informazioni che fanno sorgere un dubbio giustificato al riguardo.

(107) La Commissione dovrebbe pertanto controllare su base continuativa la situazione nell'OEB per quanto riguarda il quadro giuridico e la prassi effettiva del trattamento dei dati personali valutati dalla presente decisione. Per agevolare tale processo, l'OEB dovrebbe essere invitata a informare la Commissione degli sviluppi sostanziali rilevanti ai fini della presente decisione, per quanto concerne il trattamento dei dati personali nonché le limitazioni e le garanzie applicabili all'accesso ai dati personali da parte delle autorità pubbliche.

(108) Inoltre, al fine di consentire alla Commissione di svolgere in modo efficace la propria funzione di monitoraggio, gli Stati membri dovrebbero informarla delle eventuali azioni intraprese dalle autorità nazionali di protezione dei dati, in particolare per quanto riguarda eventuali domande o reclami presentati da interessati dell'Unione relativamente al trasferimento di dati personali dall'Unione verso l'OEB.

(109) In applicazione dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 e alla luce del fatto che il livello di protezione assicurato dal quadro giuridico dell'OEB può evolversi, la Commissione, successivamente all'adozione della presente decisione, dovrebbe riesaminare periodicamente se le constatazioni relative al livello di protezione assicurato dall'OEB continuino ad essere giustificate in fatto e in diritto. Tali valutazioni dovrebbero aver luogo almeno ogni quattro anni e dovrebbero riguardare tutti gli aspetti del funzionamento della presente decisione, compreso il funzionamento dei pertinenti meccanismi di controllo e applicazione.

(110) Per effettuare il riesame, la Commissione dovrebbe incontrare l'OEB, compresi il DPO e il DPB. A tale riunione dovrebbero poter partecipare i rappresentanti dei membri del comitato europeo per la protezione dei dati. Nel quadro del riesame la Commissione dovrebbe chiedere all'OEB di fornire informazioni complete su tutti gli aspetti pertinenti alla constatazione di adeguatezza. La Commissione dovrebbe inoltre chiedere delucidazioni in merito a qualsiasi informazione ricevuta risultata pertinente ai fini della presente decisione, compreso dall'EDPB, dalle singole autorità di protezione dei dati e dai gruppi della società civile, da relazioni pubbliche o dalle notizie diffuse dai mezzi di comunicazione o da qualsiasi altra fonte di informazioni disponibile.

(111) La Commissione dovrebbe elaborare, sulla base del riesame, una relazione pubblica da presentare al Parlamento europeo e al Consiglio.

(112) Se dalle informazioni disponibili, in particolare da quelle risultanti dal monitoraggio da parte della Commissione degli sviluppi che potrebbero incidere sul funzionamento della presente decisione ai sensi dell'articolo 45, paragrafo 4, del regolamento (UE) 2016/679 o fornite dall'OEB o dalle autorità degli Stati membri, risulta che il livello di protezione offerto dall'OEB potrebbe non essere più adeguato, la Commissione dovrebbe informarne l'OEB e richiedere che adotti misure adeguate entro un periodo di tempo specificato e ragionevole.

(113) Laddove alla scadenza di tale periodo di tempo specificato l'OEB non abbia adottato tali misure o non dimostri altrimenti in modo soddisfacente che la presente decisione continua ad essere basata su un livello di protezione adeguato, la Commissione avvierà la procedura di cui all'articolo 93, paragrafo 2, del regolamento (UE) 2016/679 al fine di sospendere o abrogare parzialmente o completamente la presente decisione.

([291]) Sentenza della Corte di giustizia del 6 ottobre 2015, *Schrems* («Schrems I»), C-362/14, ECLI:EU:C:2015:650, punto 65.

(114) In alternativa, la Commissione avvierà tale procedura al fine di modificare la presente decisione, in particolare imponendo ulteriori condizioni per i trasferimenti di dati o limitando il riconoscimento dell'adeguatezza soltanto ai trasferimenti di dati per cui continua ad essere garantito un livello di protezione adeguato.

(115) La Commissione dovrebbe inoltre valutare l'opportunità di avviare la procedura di modifica, sospensione o abrogazione della presente decisione se, nel contesto del riesame o in altro contesto, l'OEB non fornisce le informazioni o i chiarimenti necessari alla valutazione del livello di protezione offerto ai dati personali trasferiti dall'Unione o per quanto concerne la conformità alla presente decisione. A tale riguardo, la Commissione dovrebbe tener conto della misura in cui le informazioni pertinenti possono essere ottenute da altre fonti.

(116) In ragione di motivi imperativi d'urgenza debitamente giustificati, la Commissione farà ricorso alla possibilità di adottare, conformemente alla procedura di cui all'articolo 93, paragrafo 3, del regolamento (UE) 2016/679, atti di esecuzione immediatamente applicabili destinati a sospendere, abrogare o modificare la presente decisione.

7. CONSIDERAZIONI FINALI

(117) Il comitato europeo per la protezione dei dati ha pubblicato il proprio parere ([292]), del quale si è tenuto conto nell'elaborazione della presente decisione.

(118) Le misure di cui alla presente decisione sono conformi al parere del comitato istituito a norma dell'articolo 93, paragrafo 1, del regolamento (UE) 2016/679,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Ai fini dell'articolo 45 del regolamento (UE) 2016/679, l'Organizzazione europea dei brevetti garantisce un livello di protezione adeguato dei dati personali trasferiti dall'Unione all'Organizzazione europea dei brevetti.

Articolo 2

Quando, al fine di proteggere le persone con riguardo al trattamento dei loro dati personali, le autorità competenti degli Stati membri esercitano i poteri di cui all'articolo 58 del regolamento (UE) 2016/679 in relazione ai trasferimenti di dati che rientrano nell'ambito di applicazione di cui all'articolo 1, lo Stato membro interessato ne informa senza indugio la Commissione.

Articolo 3

1. La Commissione monitora costantemente l'applicazione del quadro giuridico dell'Organizzazione europea dei brevetti su cui si basa la presente decisione al fine di valutare se l'Organizzazione europea dei brevetti continui a garantire un livello di protezione adeguato ai sensi dell'articolo 1.

2. Gli Stati membri e la Commissione si informano reciprocamente dei casi in cui l'Organizzazione europea dei brevetti non garantisce il rispetto del quadro giuridico su cui si basa la presente decisione.

3. Almeno ogni quattro anni, la Commissione verifica la constatazione enunciata all'articolo 1 in base a tutte le informazioni disponibili, comprese quelle ricevute nell'ambito del riesame effettuato congiuntamente con l'Organizzazione europea dei brevetti.

([292]) Comitato europeo per la protezione dei dati, parere 7/2025 relativo al progetto di decisione di esecuzione della Commissione europea a norma del regolamento (UE) 2016-679 sulla protezione adeguata dei dati personali da parte dell'Organizzazione europea dei brevetti, disponibile all'indirizzo: https://www.edpb.europa.eu/system/files/2025-05/edpb-opinion-202507-epo-adequacydecision_en.pdf.

4. Qualora abbia indicazioni del fatto che non è più garantito un livello di protezione adeguato, la Commissione ne informa l'Organizzazione europea dei brevetti. Se necessario, la Commissione può decidere di sospendere, modificare o abrogare la presente decisione o di limitarne l'ambito di applicazione, conformemente all'articolo 45, paragrafo 5, del regolamento (UE) 2016/679.

La Commissione può inoltre sospendere, abrogare o modificare la presente decisione qualora la mancanza di cooperazione da parte dell'Organizzazione europea dei brevetti le impedisca di determinare se vi sia un impatto sulla valutazione di cui all'articolo 1 della presente decisione.

Articolo 4

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 15 luglio 2025

Per la Commissione
Michael MCGRATH
Membro della Commissione