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

Adottato il 5 maggio 2025

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Sintesi

Il 4 marzo 2025 la Commissione europea ha avviato il processo per l'adozione del suo progetto di decisione di esecuzione («progetto di decisione») sulla protezione adeguata dei dati personali da parte dell'Organizzazione europea dei brevetti (OEB o Organizzazione) ([1]).

Il 5 marzo 2025 la Commissione europea ha richiesto il parere del comitato europeo per la protezione dei dati («EDPB»). La valutazione dell'EDPB sull'adeguatezza del livello di protezione offerto dall'OEB è stata effettuata sulla base dell'esame del progetto di decisione stesso nonché dell'analisi della documentazione messa a disposizione dalla Commissione europea.

L'EDPB si è concentrato sulla valutazione del quadro giuridico e delle norme in materia di protezione dei dati applicabili all'OEB e sui mezzi di ricorso a disposizione delle persone nello Spazio economico europeo (SEE), compreso l'accesso da parte delle autorità pubbliche ai dati personali trasferiti dal SEE all'OEB.

L'EDPB ha inoltre valutato se le garanzie previste dal quadro giuridico dell'OEB siano in atto ed efficaci e ha concentrato la propria valutazione in particolare sul controllo e sull'applicazione delle norme, tenendo conto delle specificità delle organizzazioni internazionali.

Per tale lavoro l'EDPB si è basato principalmente sui criteri di riferimento per l'adeguatezza adottati dal Gruppo di lavoro Articolo 29 ([2]).

L'EDPB considera positivo il fatto che il quadro dell'OEB in materia di protezione dei dati presenta numerose analogie con il quadro dell'Unione europea in materia di protezione dei dati, anche per quanto riguarda i diritti e i principi in materia di protezione dei dati.

Ha inoltre concluso che alcuni aspetti dovrebbero essere ulteriormente chiariti e monitorati con attenzione dalla Commissione europea.

In particolare, l'EDPB invita la Commissione a chiarire che, nel contesto della struttura di governance della protezione dei dati attuata dall'OEB, il titolare del trattamento (ossia l'Ufficio europeo dei brevetti) rimane l'entità responsabile in ultima istanza delle violazioni delle norme in materia di protezione dei dati.

Per quanto riguarda i trasferimenti successivi, l'EDPB osserva che l'obbligo di non compromettere il livello di protezione non è espressamente menzionato in relazione alle cosiddette «trasmissioni» di dati personali alle autorità pubbliche degli Stati contraenti dell'OEB. L'EDPB chiede alla Commissione di chiarire questo punto e di precisare quali garanzie si applicano quando i dati personali sono trasmessi nel contesto specifico della procedura di rilascio dei brevetti.

Dato lo stretto legame tra il responsabile della protezione dei dati (RPD) e il comitato per la protezione dei dati (DPB), nonché l'importanza dei poteri di indagine, di revisione e correttivi, l'EDPB raccomanda alla Commissione di chiarire ulteriormente l'interazione tra di essi, in particolare per quanto riguarda l'esercizio dei poteri di indagine, di revisione e correttivi, nonché di chiarire il ruolo dell'RPD nella gestione delle richieste degli interessati e il suo eventuale ruolo nella procedura di reclamo dinanzi al DPB. Inoltre, l'EDPB osserva che i pareri (motivati) del DPB emanati nel contesto della procedura di reclamo rimangono non vincolanti e invita la Commissione a verificare e garantire che i poteri del DPB

([1]) Comunicato stampa all'indirizzo https://ec.europa.eu/commission/presscorner/detail/sv/ip_25_613.
([2]) Gruppo di lavoro Articolo 29, WP 254 rev.01, adottato il 28 novembre 2017, rivisto da ultimo e adottato il 6 febbraio 2018, approvato dall'EDPB.

abbiano carattere vincolante in questo contesto nonché a valutare se a tal fine possano essere previste garanzie supplementari.

L'EDPB ha inoltre analizzato il quadro giuridico dell'OEB per quanto riguarda l'accesso ai dati personali trasferiti dall'Unione all'Organizzazione e il loro utilizzo da parte delle autorità pubbliche. A tale riguardo, l'EDPB sottolinea che la valutazione dell'accesso delle pubbliche amministrazioni nel caso di specie è distinta dalla corrispondente valutazione del livello di protezione offerto da un paese terzo. Lo scenario specifico di una decisione di adeguata protezione dei dati personali da parte di un'organizzazione internazionale richiede un riesame delle norme che stabiliscono le modalità di trattamento, da parte di tale organizzazione, delle richieste di accesso delle pubbliche amministrazioni.

Per quanto riguarda gli Stati contraenti, le immunità dell'OEB sono integrate da un dovere di cooperazione. A tal fine, l'OEB può rinunciare alla propria immunità di giurisdizione ed esecuzione per rispondere alle richieste di accesso delle pubbliche amministrazioni. L'EDPB invita la Commissione a chiarire ulteriormente, in particolare per quanto riguarda le richieste di accesso a fini di applicazione della legge e di sicurezza nazionale, il modo in cui il dovere di cooperazione si collega al concetto di immunità. In tale contesto, l'EDPB invita la Commissione a chiarire altresì l'autorità e l'ambito di discrezionalità del Presidente nel decidere in merito a una richiesta di cooperazione.

Se l'OEB sceglie di soddisfare una richiesta di accesso da parte di uno Stato contraente, si applicano le prescrizioni relative alle trasmissioni. Tali norme sono applicabili a tutti gli Stati contraenti, indipendentemente dal fatto che lo Stato contraente sia uno Stato membro del SEE o si qualifichi come paese terzo dal punto di vista del diritto dell'UE in materia di protezione dei dati. L'EDPB sottolinea che i requisiti di cui al capo V del RGPD, nella misura necessaria a stabilire l'equivalenza essenziale, devono essere sufficientemente esaminati e invita la Commissione a chiarire quali garanzie si applicano in tali casi.

Indice

1. INTRODUZIONE 5
1.1 Struttura e quadro di protezione dei dati dell'OEB 5
1.2 Specificità delle organizzazioni internazionali 6
1.3 Privilegi e immunità dell'OEB 7
1.4 Governance dell'OEB in materia di protezione dei dati 7
2. ASPETTI GENERALI RELATIVI ALLA PROTEZIONE DEI DATI 8
2.1 Principi di contenuto 8
2.1.1 Nozioni 8
2.1.2 Principi di protezione dei dati 9
2.2 Diritti individuali 9
2.3 Restrizioni sui trasferimenti successivi 11
2.3.1 Trasmissioni di dati personali 11
2.4 Meccanismi procedurali e di applicazione 13
2.4.1 Responsabile della protezione dei dati e comitato per la protezione dei dati 13
2.4.2 Poteri di indagine e correttivi 14
2.4.3 Procedura di reclamo dinanzi al comitato per la protezione dei dati 16
2.4.4 Meccanismi di ricorso e arbitrato 17
3. ACCESSO AI DATI PERSONALI TRASFERITI DALL'UNIONE ALL'ORGANIZZAZIONE EUROPEA DEI BREVETTI E LORO UTILIZZO DA PARTE DELLE AUTORITÀ PUBBLICHE 19
3.1 Trattamento da parte dell'OEB delle richieste delle pubbliche amministrazioni di accesso ai dati personali 19
3.2 Limitazione dei diritti degli interessati 21
4. ATTUAZIONE E MONITORAGGIO DEL PROGETTO DI DECISIONE 22

Il comitato europeo per la protezione dei dati

visto l'articolo 70, paragrafo 1, lettera s), del 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 (in appresso «RGPD»),

visto l'accordo sullo Spazio economico europeo (SEE), in particolare l'allegato XI e il protocollo 37 dello stesso, modificato dalla decisione del comitato misto SEE n. 154/2018, del 6 luglio 2018 ([3]),

visti l'articolo 12 e l'articolo 22 del proprio regolamento interno,

HA ADOTTATO IL SEGUENTE PARERE:

1. INTRODUZIONE

1. Il capo V del RGPD stabilisce le condizioni per i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale. I trasferimenti di dati personali sono ammessi sulla base di una decisione di adeguatezza della Commissione europea (articolo 45 RGPD) o, in mancanza di tale decisione di adeguatezza, nel caso in cui il titolare del trattamento o il responsabile del trattamento fornisca garanzie adeguate, compresi diritti azionabili e mezzi di ricorso per l'interessato (articolo 46 RGPD). In mancanza di una decisione di adeguatezza o di garanzie adeguate, il trasferimento o il complesso di trasferimenti verso un paese terzo o un'organizzazione internazionale è ammesso solo a determinate condizioni (articolo 49 RGPD).

2. L'EDPB ricorda che le decisioni di adeguatezza garantiscono la protezione continua dei dati personali trasferiti dal SEE verso paesi terzi e costituiscono un solido strumento di trasferimento per garantire la salvaguardia dei diritti dell'interessato quando i dati sono trasferiti al di fuori del SEE.

3. In particolare, l'EDPB accoglie con favore l'iniziativa della Commissione di lavorare sulla prima decisione di adeguatezza per un'organizzazione internazionale e sottolinea l'importanza di tale decisione per dimostrare come si possa riconoscere che il quadro giuridico di organizzazioni internazionali garantisce un livello di protezione adeguato ai sensi dell'articolo 45 RGPD.

4. L'EDPB coglie l'occasione per incoraggiare la Commissione a proseguire il dialogo con le organizzazioni internazionali al fine di elaborare, ampliare e moltiplicare questo tipo di decisioni di adeguatezza insieme a quelle relative ai paesi terzi.

1.1 Struttura e quadro di protezione dei dati dell'OEB

5. L'Organizzazione europea dei brevetti, con sede a Monaco di Baviera, è un'organizzazione intergovernativa istituita dalla Convenzione sul brevetto europeo (CBE) ([4]). Conta 39 Stati contraenti ed è dotata di personalità giuridica. È composta da due organi principali: l'Ufficio europeo dei brevetti (Ufficio), che funge da braccio esecutivo, e il Consiglio di amministrazione, che esercita poteri legislativi per conto dell'OEB ed è responsabile delle questioni in materia di politiche (articolo 33 CBE).

([3]) Nel presente parere, con il termine «Stati membri» si intendono gli «Stati membri del SEE».
([4]) Considerando 7 del progetto di decisione.

6. La competenza principale dell'OEB è il rilascio di brevetti europei, compito svolto dall'Ufficio sotto la supervisione del Consiglio di amministrazione.

7. Il Presidente rappresenta l'OEB ed è il capo dell'Ufficio, che comprende vari servizi. Il Presidente è responsabile della gestione delle operazioni dell'Ufficio e delle questioni disciplinari e risponde al Consiglio di amministrazione. Il Consiglio di amministrazione è composto da rappresentanti degli Stati contraenti, supervisiona le questioni politiche e le attività dell'Ufficio.

8. Il 30 giugno 2021 l'OEB ha adottato le norme in materia di protezione dei dati (*Data Protection Rules*, DPR) che attuano gli articoli 1 *ter* e 32 *bis* dello statuto ([5]) e sono applicabili al trattamento dei dati personali da parte dell'Ufficio ([6]).

9. Le DPR sono integrate da strumenti emanati dal Presidente, in particolare circolari, istruzioni amministrative interne e decisioni (come la decisione sui paesi e le entità che garantiscono un'adeguata protezione dei dati (17 novembre 2022) e la «*circolare n. 420 di attuazione dell'articolo 25 delle norme in materia di protezione dei dati (DPR) sulla limitazione dei diritti degli interessati*»). Tutti questi strumenti sono giuridicamente vincolanti ([7]).

10. Le DPR sono ulteriormente integrate da documenti operativi emessi dal responsabile della protezione dei dati, che specificano prescrizioni e procedure più dettagliate per il trattamento dei dati personali (articolo 1, paragrafo 2, lettera c) DPR). Tali documenti operativi fanno parte del quadro giuridico dell'OEB in materia di protezione dei dati e sono pertanto giuridicamente vincolanti e sono a disposizione degli interessati sul sito web dell'OEB.

1.2 Specificità delle organizzazioni internazionali

11. Ai sensi dell'articolo 4, punto 26, RGPD, si intende per organizzazione internazionale (OI) «*un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati*». Secondo il diritto internazionale, lo status delle organizzazioni internazionali è simile a quello degli Stati sovrani; tuttavia, in base al principio dell'immunità funzionale, le organizzazioni internazionali godono di privilegi e immunità solo nella misura necessaria all'esercizio delle funzioni per le quali sono state create ([8]). I «privilegi» comprendono generalmente esenzioni dal diritto sostanziale di uno Stato (ad esempio esenzioni fiscali e doganali), mentre le «immunità» sono esenzioni dai procedimenti giudiziari, dall'esecuzione e dalle misure di esecuzione.

([5]) Lo statuto disciplina gli aspetti relativi al personale dell'OEB, compresi i diritti e gli obblighi del personale. Cfr. a questo proposito l'articolo 33 CBE. La CBE è disponibile al seguente indirizzo: https://link.epo.org/web/EPC_17th_edition_2020_en.pdf.

([6]) Il trattamento dei dati personali effettuato dal Consiglio di amministrazione dell'OEB è disciplinato dal documento *Administrative Council Data Protection Rules* (AC DPR), mentre il trattamento dei dati personali effettuato dal Comitato ristretto è disciplinato dal documento *Select Committee Data Protection Rules* (SC DPR). L'AC DPR e l'SC DPR stabiliscono rispettivamente l'applicazione delle DPR al trattamento dei dati personali effettuato dal Consiglio di amministrazione e dal Comitato ristretto, con le necessarie modifiche. L'articolo 145 CBE chiarisce il ruolo del Comitato ristretto.

([7]) Articolo 10 CBE, articolo 1, paragrafo 2, lettera a), DPR e articolo 3, lettera y), DPR.

([8]) Christopher Kuner: *International Organizations and the EU General Data Protection Regulation*, University of Cambridge Faculty of Law Legal Studies Research Paper Series, Paper 20/2018.

12. Le fonti dei privilegi e delle immunità delle organizzazioni internazionali possono essere: i trattati multilaterali, gli accordi internazionali che istituiscono l'organizzazione internazionale, gli accordi di sede con lo Stato ospitante, il diritto e la legislazione nazionale. I privilegi e le immunità sono generalmente riconosciuti dagli Stati che sono membri delle organizzazioni, salvo che i paesi terzi non abbiano riconosciuto esplicitamente o implicitamente l'organizzazione internazionale nel diritto nazionale. Tuttavia, l'immunità dalla giurisdizione nazionale non è assoluta e richiede che le persone dispongano di mezzi alternativi ragionevoli per proteggere efficacemente i loro diritti ([9]).

1.3 Privilegi e immunità dell'OEB

13. I privilegi e le immunità di cui gode l'OEB sono disciplinati dal «*Protocol on Privileges and Immunities of the European Patent Organisation*» (PPI, Protocollo sui privilegi e sulle immunità dell'Organizzazione europea dei brevetti) e riguardano, tra l'altro, la sede dell'OEB (articolo 1 PPI); l'inviolabilità degli archivi (articolo 2 PPI); la giurisdizione e l'esecuzione (articolo 3, paragrafo 1, lettera a), PPI), gli edifici e i beni dell'OEB: tranne nella misura in cui possa essere temporaneamente necessario in relazione alla prevenzione e alle indagini sugli incidenti che coinvolgono veicoli a motore appartenenti o gestiti per conto dell'Organizzazione (articolo 3, paragrafo 3, PPI); esenzione fiscale (articolo 4 PPI).

14. Le immunità dell'OEB sono integrate da un dovere di cooperazione tra l'OEB e le autorità pubbliche degli Stati contraenti, come stabilito all'articolo 20 PPI. Inoltre, ai sensi dell'articolo 19, paragrafo 2, il Presidente dell'Ufficio europeo dei brevetti ha il dovere di revocare l'immunità qualora ritenga che tale immunità impedisca il normale corso della giustizia e che sia possibile rinunciare a tale immunità senza compromettere gli interessi dell'Organizzazione.

1.4 Governance dell'OEB in materia di protezione dei dati

15. Ai sensi dell'articolo 3, lettera g), DPR, l'Ufficio europeo dei brevetti agisce in qualità di titolare del trattamento ([10]). Il quadro giuridico dell'OEB in materia di protezione dei dati prevede la possibilità per il titolare del trattamento di identificare le unità operative in qualità di «titolari del trattamento delegati» (articolo 28, paragrafo 3, DPR). Ai sensi dell'articolo 3, lettera h), DPR, per «*titolare del trattamento delegato si intende l'unità operativa, rappresentata dal suo capo, che garantisce che tutte le operazioni di trattamento di dati personali effettuate all'interno dell'unità operativa siano conformi alle presenti norme. La persona che rappresenta l'unità è un dirigente di alto livello, di norma almeno un direttore principale*».

([9]) Corte EDU, *Waite e Kennedy/Germania*, domanda n. 26083/94, sentenza del 18 febbraio 1999, punti da 67 a 73.
([10]) L'articolo 28 DPR specifica ulteriormente la titolarità all'interno dell'OEB.

16. L'EDPB osserva che questa struttura di governance interna è comune nel contesto delle organizzazioni internazionali ([11]), date le dimensioni e la natura del loro lavoro. Analogamente, le imprese beneficiano della presenza di una struttura interna a sostegno del rispetto delle norme in materia di protezione dei dati ([12]).

17. Tuttavia, l'EDPB osserva che la responsabilità finale in caso di violazione delle norme sulla protezione dei dati dovrebbe rimanere in capo al titolare del trattamento (ossia l'Ufficio europeo dei brevetti) ([13]). Alla luce di quanto precede, l'EDPB invita la Commissione a chiarire ulteriormente questo punto.

2. ASPETTI GENERALI RELATIVI ALLA PROTEZIONE DEI DATI

2.1 Principi di contenuto

18. Il capitolo 3 dei criteri di riferimento per l'adeguatezza è dedicato ai «principi di contenuto» e fa riferimento alle nozioni e ai principi di base in materia di protezione dei dati. Il sistema di un paese terzo o di un'organizzazione internazionale deve comprendere tali nozioni e principi di base per garantire un livello di protezione dei dati personali sostanzialmente equivalente a quello garantito dal diritto dell'UE. Pur non dovendo necessariamente riprendere la terminologia del RGPD, tali nozioni e principi dovrebbero rispecchiare le nozioni racchiuse nel diritto europeo in materia di protezione dei dati ed essere coerenti con esse. I criteri di riferimento per l'adeguatezza fanno riferimento alle seguenti nozioni importanti: «dati personali», «trattamento di dati personali», «titolare del trattamento», «responsabile del trattamento», «destinatario» e «dati sensibili».

19. L'EDPB accoglie con favore il riconoscimento dei diritti alla tutela della vita privata e alla protezione dei dati come diritti fondamentali ai sensi del RGPD.

2.1.1 Nozioni

20. L'EDPB riconosce che la terminologia utilizzata nel quadro giuridico dell'OEB in materia di protezione dei dati è coerente con quella del quadro giuridico dell'UE in materia di protezione dei dati. Questo allineamento è un fattore positivo che, pur non essendo un prerequisito per l'equivalenza, merita di essere riconosciuto.

21. Per quanto riguarda le nozioni di «titolare del trattamento delegato» e di «unità operativa», e le loro conseguenze pratiche, l'EDPB rinvia alla precedente sezione 1.4.

([11]) Ad esempio, il regolamento di Eurocontrol sulla protezione dei dati fa riferimento ai «titolari del trattamento interni», cfr. https://www.eurocontrol.int/sites/default/files/2024-05/eurocontrol-regulation-personal-data-protection-2024.pdf; la BEI utilizza il termine «titolari del trattamento» sia per i titolari del trattamento delegati sia per la BEI, ma il testo fa spesso riferimento ai «titolari del trattamento pertinenti» chiarendo che si tratta di un'entità specifica all'interno della BEI, cfr. https://www.eib.org/attachments/lucalli/20220237_data_protection_rules_implementing_eu_regulation_en.pdf.

([12]) Linee guida 7/2020 dell'EDPB sui concetti di titolare del trattamento e di responsabile del trattamento di cui al RGPD, versione 2.1, adottate il 7 luglio 2021.

([13]) Ibidem, punti 17 e 18.

2.1.2 Principi di protezione dei dati

22. I principi di protezione dei dati di cui all'articolo 4, paragrafo 2, e all'articolo 6 DPR sono molto simili a quelli di cui, rispettivamente, all'articolo 5 e all'articolo 6, paragrafo 4, RGPD. Analogamente, le basi giuridiche per il trattamento di cui agli articoli 5, 7, 11 e 12 DPR rispecchiano le basi giuridiche di cui all'articolo 6 RGPD e le condizioni di cui agli articoli 9 e 10 RGPD ([14]).

23. Ai sensi dell'articolo 11, paragrafo 2, DPR, categorie particolari di dati personali possono essere trattate in condizioni molto simili a quelle previste dall'articolo 9 RGPD, ad eccezione di alcuni casi derivanti dalla natura dell'OEB. Ai sensi dell'articolo 11, paragrafo 2, lettera f), DPR, ad esempio, tali dati possono essere trattati quando sono necessari per una finalità specifica relativa all'esecuzione di un compito svolto nell'esercizio delle attività ufficiali dell'Organizzazione o nell'esercizio legittimo dei pubblici poteri di cui è investito il titolare del trattamento.

24. In tali casi, tuttavia, l'articolo 11, paragrafo 2, lettera f), DPR prevede misure specifiche per garantire che il livello di protezione delle categorie particolari di dati personali non sia compromesso.

25. L'EDPB accoglie con favore il fatto che, in relazione al principio di limitazione delle finalità, la compatibilità di ulteriori finalità sia intesa in modo analogo sia nell'articolo 4, paragrafo 2, lettera b), e nell'articolo 6 DPR, sia nell'articolo 5, paragrafo 1, lettera b), e nell'articolo 6, paragrafo 4, RGPD.

26. Inoltre, l'EDPB accoglie con favore l'inclusione del principio di responsabilità nell'articolo 4, paragrafo 1, DPR e delle misure necessarie per dimostrare la conformità, quali la tenuta dei registri (articolo 32 DPR), gli obblighi di notifica delle violazioni dei dati (articolo 34 DPR), la valutazione degli impatti sulla protezione dei dati (articolo 38 DPR) nonché l'inclusione della tutela della vita privata fin dalla progettazione e per impostazione predefinita (articolo 27, paragrafi 1 e 2, DPR), che garantiscono anche il rispetto dei principi di minimizzazione dei dati e di necessità. L'EDPB rileva con soddisfazione che tali principi e obblighi sono molto simili a quelli stabiliti nell'ambito del RGPD.

27. Inoltre, l'EDPB accoglie con favore il fatto che l'articolo 4, paragrafo 1, DPR preveda che il titolare del trattamento attui attivamente e costantemente misure volte a garantire la protezione dei dati personali nelle sue attività di trattamento, rendendolo responsabile del rispetto della normativa in materia di protezione dei dati e imponendogli di dimostrare in qualsiasi momento tale conformità agli interessati.

2.2 Diritti individuali

28. L'EDPB accoglie con favore il fatto che le DPR conferiscano alle persone fisiche gli stessi diritti previsti dal RGPD (articoli da 12 a 22), 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). Allo stesso modo, il diritto di essere informati sulla limitazione dei diritti dell'interessato (articolo 23, paragrafo 2, lettera h) RGPD) è riconosciuto dall'articolo 7 della circolare n. 420 emanata dal Presidente dell'OEB.

([14]) Cfr. i considerando da 26 a 29 del progetto di decisione.

29. Analogamente all'articolo 23 RGPD, l'articolo 25 DPR stabilisce che disposizioni giuridiche specifiche nell'ambito del quadro giuridico dell'OEB possono limitare l'applicazione dei diritti di cui agli articoli da 18 a 25 DPR e prevede il contenuto minimo delle misure che prevedono le limitazioni. Tale contenuto minimo rispecchia quello richiesto dal RGPD. Inoltre, ogni valutazione della necessità di una limitazione deve essere debitamente documentata.

30. Finora l'OEB ha attuato questa disposizione mediante la circolare n. 420, che chiarisce quali diritti possono essere limitati e per quali obiettivi. Chiarisce inoltre che la limitazione è temporanea e che spetta al titolare del trattamento stabilire se, alla luce delle circostanze pertinenti, la limitazione sia applicabile. A tal fine, il titolare del trattamento effettua una verifica della necessità e della proporzionalità caso per caso, che deve essere documentata e comunicata all'RPD dell'OEB. L'RPD ha il potere di chiedere il riesame di una limitazione e il titolare del trattamento deve informare per iscritto dell'esito del riesame.

31. L'EDPB rileva con soddisfazione che, ai sensi dell'articolo 25, paragrafi 2 e 4, DPR e dell'articolo 7 della circolare n. 420, gli interessati devono essere informati delle limitazioni, a meno che ciò non ne annulli l'effetto (in linea con l'articolo 23 RGPD e l'articolo 25 EUDPR), e del loro diritto di consultare l'RPD al fine di contestare le limitazioni e i loro diritti ai sensi degli articoli 9 e 50 DPR (articolo 25, paragrafo 3, lettera b), DPR). In tale contesto, l'EDPB accoglie con favore il fatto che le informazioni sulle limitazioni dei diritti degli interessati siano disponibili sul sito web dell'OEB, in conformità dell'articolo 7 della circolare n. 420.

32. Inoltre, l'EDPB osserva che, in considerazione dei compiti dell'OEB, esistono diverse limitazioni dei diritti degli interessati. L'OEB, ad esempio, ha il dovere di mantenere il registro europeo dei brevetti, dove sono pubblicati alcuni dati personali definiti per legge. Allo stesso modo, il diritto di rettifica e di cancellazione sono limitati: l'OEB non può procedere alla rettifica delle informazioni - compresi i dati personali – contenute nei documenti utilizzati nella procedura di rilascio dei brevetti (come invece avviene per i documenti relativi a procedimenti ufficiali e legali, quali una dichiarazione di rivendicazione o una dichiarazione di risposta) e l'OEB deve attenersi a specifici periodi di conservazione e requisiti di pubblicazione per alcuni documenti utilizzati nella procedura di rilascio dei brevetti (articolo 129, lettera a), CBE).

33. L'EDPB osserva che le limitazioni dei diritti degli interessati previste dall'OEB riguardano quanto strettamente necessario e proporzionato per garantire il corretto funzionamento della procedura di rilascio dei brevetti, rispettando in tal modo l'essenza dei diritti fondamentali e della libertà degli interessati e i requisiti di necessità e proporzionalità stabiliti nella Carta dei diritti fondamentali dell'Unione europea (Carta) e nella Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

2.3 Restrizioni sui trasferimenti successivi

34. I criteri di riferimento per l'adeguatezza ai sensi del RGPD chiariscono che il livello di tutela delle persone fisiche i cui dati sono trasferiti a norma di una decisione di adeguatezza non deve essere compromesso dal trasferimento successivo e pertanto ulteriori trasferimenti «dovrebbero essere consentiti soltanto quando anche l'ulteriore destinatario (ossia il destinatario del trasferimento successivo) è soggetto a norme (comprese le norme contrattuali) che assicurano un livello di protezione adeguato e prevedono il rispetto delle istruzioni pertinenti durante il trattamento dei dati per conto del titolare del trattamento» ([15]). Mentre le DPR distinguono tra le cosiddette «trasmissioni di dati personali» e i «trasferimenti di dati personali» e prevedono regole diverse per queste due categorie di trasferimenti ([16]), l'EDPB sottolinea che il requisito di non compromettere il livello di protezione si applica a tutti i trasferimenti successivi di dati personali trasferiti dall'UE, indipendentemente dalla terminologia utilizzata.

35. L'EDPB osserva che ai «trasferimenti di dati personali» (quali definiti all'articolo 3, lettera t), DPR) si applicano norme molto simili a quelle del capo V del RGPD al fine di garantire che il livello di protezione garantito dalle DPR non sia compromesso (articoli 9 e 10 DPR).

36. L'EDPB accoglie con favore questo stretto allineamento con il capo V del RGPD e prende atto con soddisfazione del riferimento contenuto negli orientamenti sul trasferimento del responsabile della protezione dei dati alle linee guida dell'EDPB e agli sviluppi nel quadro dell'Unione ([17]).

37. Alla luce di quanto precede, l'EDPB ha concentrato la sua valutazione sulle norme applicabili all'altra categoria di trasferimenti ai sensi delle DPR, le «trasmissioni di dati personali».

2.3.1 Trasmissioni di dati personali

38. Ai sensi dell'articolo 3, lettera s), DPR, per «trasmissione di dati personali» si intende «la comunicazione, la diffusione o la messa a disposizione in altro modo, anche mediante concessione dell'accesso, di dati personali a una parte dell'Organizzazione europea dei brevetti o a un ufficio nazionale della proprietà industriale o a un'altra autorità pubblica di uno Stato contraente della Convenzione sul brevetto europeo alle condizioni di cui all'articolo 8».

([15]) Gruppo di lavoro Articolo 29, WP 254 rev.01, adottato il 28 novembre 2017, rivisto da ultimo e adottato il 6 febbraio 2018, approvato dall'EDPB, capitolo 3, A.9.
([16]) Cfr. i considerando da 62 a 72 del progetto di decisione.
([17]) EPO transmission and transfer of personal data, Explanatory Note (Trasmissione e trasferimento di dati personali da parte dell'OEB, nota esplicativa), versione di gennaio 2024, parte 3.2 (pag. 9).

39. L'articolo 8, paragrafo 1, DPR stabilisce che la trasmissione di dati personali a un'autorità pubblica di uno Stato contraente dell'OEB può avvenire se i dati sono necessari all'adempimento dei compiti di tale autorità pubblica e se la trasmissione è compatibile con i compiti e il funzionamento dell'OEB ([18]). L'articolo 8, paragrafo 2, DPR consente la trasmissione di dati personali a un ufficio nazionale per la proprietà industriale di uno Stato contraente dell'OEB se i dati sono necessari all'esercizio della competenza del destinatario e l'esercizio di pubblici poteri e se il trattamento è necessario all'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, il che include il trattamento necessario per la gestione e il funzionamento dell'OEB. Tali trasmissioni si svolgono nell'ambito della procedura di rilascio dei brevetti prevista dalla CBE e dal TCB ([19]).

40. I destinatari devono dimostrare la necessità che i dati siano trasmessi per una finalità specifica derivante dagli obblighi di cooperazione dell'OEB con lo Stato contraente, e il titolare del trattamento – qualora possano essere lesi i legittimi interessi dell'interessato - deve dimostrare che è proporzionato trasmettere i dati personali per tale finalità specifica, dopo aver ponderato i diversi interessi in gioco (articolo 8, paragrafi 3 e 4, DPR).

41. Al fine di fornire garanzie adeguate come strumenti per le trasmissioni, negli strumenti applicabili, quali memorandum d'intesa o accordi amministrativi ([20]), dovrebbero essere inserite disposizioni specifiche in materia di protezione dei dati. L'RPD dell'OEB ha elaborato clausole tipo di protezione dei dati per i memorandum d'intesa che prevedono, tra l'altro, principi di protezione dei dati, ad esempio la limitazione delle finalità, i diritti degli interessati, nonché una vigilanza indipendente e adeguati meccanismi di applicazione ([21]). L'EDPB riconosce l'esistenza di tali garanzie, ma osserva che il requisito di non compromettere il livello di protezione non è specificamente menzionato in relazione alle trasmissioni, né nell'articolo 8 DPR, né nella nota esplicativa dell'OEB sulla trasmissione e il trasferimento di dati personali, né nel progetto di decisione di adeguatezza. L'EDPB osserva che, al contrario, questo requisito è espressamente menzionato nel contesto dei trasferimenti ([22]) e chiede alla Commissione di chiarire questo punto.

42. Inoltre, sulla base delle ulteriori spiegazioni fornite dalla Commissione, l'EDPB ha compreso che l'obbligo di fornire adeguate garanzie come strumenti per le trasmissioni non si applica nel caso in cui il destinatario sia un ufficio nazionale della proprietà industriale. Di conseguenza, non è del tutto chiaro all'EDPB quali garanzie in materia di protezione dei dati si applichino quando i dati personali sono trasmessi nel contesto della procedura di rilascio dei brevetti. L'EDPB invita pertanto la Commissione a chiarire anche questo punto.

([18]) Cfr. il considerando 63 del progetto di decisione; ciò potrebbe essere finalizzato alla cooperazione attraverso procedure di consultazione, al distacco e all'invio di esperti, alla fornitura di informazioni sul personale dell'OEB ai fini della determinazione delle prestazioni sociali, degli adempimenti fiscali, ecc.

([19]) Cfr. il considerando 62, nota a più pagina 165, del progetto di decisione e GU OEB 2021, A98 — Decision of the President of the European Patent Office dated 13 December 2021 concerning the processing of personal data in patent-grant and related proceedings (Decisione del Presidente dell'Ufficio europeo dei brevetti del 13 dicembre 2021 relativa al trattamento dei dai personali nell'ambito del rilascio dei brevetti e dei procedimenti connessi).

([20]) EPO transmission and transfer of personal data, Explanatory Note (Trasmissione e trasferimento di dati personali da parte dell'OEB, nota esplicativa), versione del gennaio 2024, pag. 6.

([21]) Overview of the requirements of the EPO's model data protection clause for Memoranda of Understanding (Panoramica dei requisiti della clausola tipo dell'OEB sulla protezione dei dati per i memorandum d'intesa), versione del giugno 2024.

([22]) Cfr. il considerando 67 del progetto di decisione.

2.4 Meccanismi procedurali e di applicazione

43. Secondo i criteri di riferimento per l'adeguatezza ([23]) e la giurisprudenza pertinente della CGUE ([24]), un sistema di protezione dei dati sostanzialmente equivalente al modello dell'Unione europea deve prevedere: i) un'autorità indipendente, che dovrebbe supervisionare e applicare le leggi in materia di protezione dei dati, con il potere di indagare e intervenire senza influenze esterne. I sistemi di protezione dei dati devono garantire ii) che i titolari e i responsabili del trattamento dei dati siano responsabili e consapevoli delle loro responsabilità, mentre gli interessati siano informati dei loro diritti. Dovrebbero essere previste sanzioni e procedure di verifica efficaci per garantire il rispetto delle norme; iii) che i titolari e i responsabili del trattamento dei dati dimostrino la conformità, attraverso misure quali le valutazioni d'impatto sulla protezione dei dati, i registri delle attività di trattamento e la nomina dei responsabili della protezione dei dati. Inoltre, iv) il sistema di protezione dei dati deve fornire sostegno e assistenza ai singoli interessati nell'esercizio dei loro diritti e meccanismi di ricorso adeguati.

44. Per quanto riguarda il principio di responsabilità che copre i punti ii) e iii) del paragrafo precedente, l'EDPB rinvia alla precedente sezione 2.1.2.

45. Nelle sezioni che seguono, l'EDPB ha concentrato la sua valutazione sull'esistenza di un'autorità indipendente e di un adeguato meccanismo di ricorso.

1.

2.

2.1

2.2

2.3

2.4

2.4.1 Responsabile della protezione dei dati e comitato per la protezione dei dati

46. Il sistema presentato dall'OEB istituisce due organismi distinti responsabili del controllo del rispetto delle norme in materia di protezione dei dati: il responsabile della protezione dei dati e il comitato per la protezione dei dati (articolo 32 *bis* dello statuto).

47. Il responsabile della protezione dei dati dell'OEB, oltre a svolgere il ruolo tradizionale di RPD ai sensi delle DPR, detiene anche poteri di indagine ai sensi dell'articolo 43 DPR.

48. Il ruolo del DPB è quello di garantire un controllo indipendente, efficace e imparziale delle norme in materia di protezione dei dati. Gli interessati hanno il diritto di presentare un reclamo dinanzi al DPB in caso di disaccordo con una decisione o di rifiuto implicito di una richiesta di riesame da parte di un titolare del trattamento delegato (articolo 50 DPR).

([23]) Gruppo di lavoro Articolo 29, WP 254 rev.01, adottato il 28 novembre 2017, rivisto da ultimo e adottato il 6 febbraio 2018, approvato dall'EDPB, capitolo 3, C.
([24]) CGUE, sentenza del 6 ottobre 2015, causa C-362/14, *Maximillian Schrems/Data Protection Commissioner* («Schrems»).

49. Sebbene questa doppia struttura, giustificata dalla natura dell'OEB, non sia intrinsecamente preoccupante o problematica, è essenziale che entrambi gli organi operino in piena indipendenza per garantire un controllo e un'applicazione efficaci e che dispongano di tutti i poteri necessari per adempiere i loro compiti.

50. A questo proposito, l'EDPB ha concentrato la sua valutazione sull'effettiva indipendenza di questi organi di controllo e sui loro poteri. Per quanto riguarda l'indipendenza, l'EDPB accoglie con favore non solo la formulazione a sostegno di questo principio negli articoli pertinenti, ma anche le garanzie aggiuntive previste.

51. In tale contesto, l'EDPB ha esaminato le norme che disciplinano la nomina, la rimozione e la revoca dell'RPD e del DPB, in particolare l'obbligo per il Presidente di consultare il DPB prima di qualsiasi proposta di rimozione o revoca dell'RPD.

52. L'EDPB ritiene che tale consultazione preventiva costituisca una potenziale garanzia per l'indipendenza dell'RPD, ma la natura e le implicazioni di tale consultazione rimangono poco chiare. Pertanto, l'EDPB invita la Commissione a chiarire ulteriormente questo punto e a prendere in considerazione la possibilità di monitorare, durante futuri riesami, che nella pratica l'RPD non sia rimosso o penalizzato dal titolare del trattamento per l'esercizio delle sue funzioni.

53. L'EDPB osserva che, ai sensi dell'articolo 47 DPR, il DPB ha una funzione di controllo e di consulenza, in quanto consiglia il titolare del trattamento e i titolari del trattamento delegati in relazione all'applicazione degli articoli 38 e 39 DPR, fornisce consulenza sulla revoca del responsabile della protezione dei dati ai sensi dell'articolo 48, paragrafo 2, DPR e fornisce un parere sull'uso del meccanismo di ricorso legale ai sensi dell'articolo 50.

54. Per quanto riguarda la nomina dei membri del comitato per la protezione dei dati, l'EDPB osserva che, a norma dell'articolo 48, paragrafo 1, DPR, il comitato per la protezione dei dati è composto da tre esperti esterni nel settore della protezione dei dati nominati dal Presidente dell'Ufficio, vale a dire un presidente e altri due membri, uno dei quali funge da vicepresidente. Ai sensi dell'articolo 48, paragrafo 2, DPR, il presidente, gli altri due membri e i supplenti del DPB devono possedere le qualifiche richieste per la nomina a funzioni giurisdizionali o essere professionisti della protezione dei dati con comprovata competenza ed esperienza nel settore.

55. L'EDPB accoglie con favore il fatto che le norme per la selezione dei membri dell'organo di controllo richiedano competenze in materia di protezione dei dati e incoraggia la Commissione a monitorare che i membri del DPB selezionati per le loro qualifiche dispongano del livello necessario di competenze in materia di protezione dei dati, considerata la sua importanza per la funzione di controllo.

2.4.2 Poteri di indagine e correttivi

56. In tale contesto, la CGUE ha chiarito che i poteri delle autorità di controllo costituiscono mezzi necessari all'adempimento dei loro compiti e che esse dovrebbero godere, segnatamente, di poteri investigativi, come quello di raccogliere qualsiasi informazione necessaria all'esercizio della loro funzione di controllo, di poteri effettivi d'intervento, come quello di vietare a titolo provvisorio o definitivo un trattamento di dati o, ancora, del potere di promuovere azioni giudiziarie ([25]).

([25]) CGUE, sentenza del 6 ottobre 2015, causa C-362/14, *Maximillian Schrems/Data Protection Commissioner* («Schrems»), punto 43.

57. Ai sensi dell'articolo 43, paragrafo 1, lettera d), l'RPD può svolgere audit sulla protezione dei dati e indagini (condotte sotto forma di ispezioni o interrogazioni ad hoc in materia di protezione dei dati) ([26]). Secondo la nota «*Data Protection Oversight*» (Controllo della protezione dei dati) ([27]), che illustra in dettaglio l'articolo 43 DPR, l'RPD, in consultazione con il DPB, prepara un piano annuale di controllo della protezione dei dati («piano») e lo sottopone all'approvazione del Presidente dell'OEB. Il piano approvato viene presentato al DPB per informazione. Il DPB può, in qualsiasi momento, formulare suggerimenti sui settori in cui l'Ufficio dovrebbe effettuare un audit della protezione dei dati.

58. Ai sensi dell'articolo 43, paragrafo 1, lettera i), DPR, l'RPD deve rispondere alle richieste del comitato per la protezione dei dati e collaborare e consultarsi con quest'ultimo su richiesta dello stesso o di propria iniziativa. Ai sensi dell'articolo 43, paragrafo 1, lettera j), DPR, l'RPD deve agevolare la cooperazione tra il comitato per la protezione dei dati e l'Ufficio per quanto riguarda, tra l'altro, le indagini in materia di protezione dei dati, la gestione dei reclami, le valutazioni d'impatto sulla protezione dei dati e le consultazioni preliminari. L'RPD deve inoltre trasmettere al DPB informazioni sulle nuove misure amministrative e sulle norme interne relative al trattamento dei dati personali.

59. L'RPD compila una relazione sulle indagini e sugli audit effettuati e, qualora sia individuata una non conformità alle norme in materia di protezione dei dati, la relazione include le risultanze, le conclusioni e le raccomandazioni (comprese le misure correttive).

60. In particolare, secondo la nota «*Data Protection Oversight*», le raccomandazioni possono includere «misure preventive, di mitigazione o correttive» per il titolare del trattamento in caso di irregolarità o di non conformità. L'RPD può raccomandare di rendere le operazioni di trattamento conformi alle DPR, di soddisfare le richieste degli interessati di esercitare i loro diritti ai sensi delle DPR, di comunicare una violazione dei dati personali all'interessato o agli interessati, di sospendere una particolare operazione di trattamento dei dati o di sospendere il flusso di dati verso destinatari specifici ([28]).

([26]) I poteri di indagine dell'RPD sono ulteriormente specificati nel documento «*Data Protection Oversight - How the Data Protection Office conduct DP Audits and DP Inspections*» (Controllo della protezione dei dati – Modalità di svolgimento degli audit e delle ispezioni in materia di protezione dei dati da parte del responsabile della protezione dei dati), disponibile sul sito web dell'OEB al seguente indirizzo: https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-data-protection-oversight-mechanism.pdf.

([27]) «*Data Protection Oversight – How the Data Protection Office conduct DP Audits and DP Inspections*» (Controllo della protezione dei dati - Modalità di svolgimento degli audit e delle ispezioni in materia di protezione dei dati da parte del responsabile della protezione dei dati), disponibile sul sito web dell'OEB al seguente indirizzo https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-data-protection-oversight-mechanism.pdf.

([28]) Ibidem.

61. In linea con la nota «*Data Protection Oversight*» e con la decisione del Presidente dell'Ufficio del 12 luglio 2024 (29), le conclusioni e le raccomandazioni possono diventare vincolanti (previa convalida del comitato) e devono essere attuate dal titolare del trattamento. Secondo la nota *Data Protection Oversight*», che fornisce ulteriori dettagli sulle norme contenute nell'articolo 43, paragrafo 1, lettere i) e j), DPR, il DPB ha il potere di formulare osservazioni sulle conclusioni e sulle raccomandazioni e di chiedere modifiche, che l'RPD è tenuto ad attuare. Inoltre, l'RPD ha l'autorità di avviare ispezioni di follow-up o di estendere la portata delle ispezioni in materia di protezione dei dati e di raccomandare l'avvio di un'indagine amministrativa al fine di accertare se siano necessarie misure disciplinari o di altro tipo.

62. Tenuto conto dello stretto legame tra l'RPD e il DPB nonché dell'importanza dei poteri di indagine, di revisione e correttivi, l'EDPB raccomanda alla Commissione di chiarire ulteriormente l'interazione tra di essi, in particolare per quanto riguarda l'esercizio dei poteri di indagine, di revisione e correttivi, nonché di chiarire il ruolo dell'RPD nella gestione delle richieste degli interessati (articolo 43, paragrafo 1, lettera k), DPR) e il suo eventuale ruolo nella procedura di reclamo dinanzi al DPB i ai sensi dell'articolo 50 DPR. In particolare, l'EDPB invita la Commissione a monitorare che sia chiaramente distinto nella pratica quando l'RPD agisce per proprio conto (svolgendo il suo ruolo e la sua funzione in qualità di responsabile della protezione dei dati) e quando agisce per conto del DPB per sostenere quest'ultimo nello svolgimento delle sue funzioni di controllo. Ciò fornirebbe ulteriore chiarezza sulla struttura di controllo e sui ruoli dell'RPD e del DPB.

2.4.3 Procedura di reclamo dinanzi al comitato per la protezione dei dati

63. L'EDPB osserva che gli interessati hanno il diritto di presentare un reclamo al comitato per la protezione dei dati che lo tratta conformemente alla procedura di cui all'articolo 50 DPR e al regolamento interno di cui all'allegato 1 delle DPR.

64. In particolare, dopo aver esaminato il reclamo, il DPB emana un parere motivato destinato al titolare del trattamento, in cui può raccomandare la concessione di un risarcimento dei danni materiali o immateriali.

65. Ai sensi dell'articolo 50, paragrafo 4, DPR, i pareri motivati del DPB (di seguito anche pareri) non sono vincolanti per il titolare del trattamento, che può decidere di non seguirli. In tal caso, il titolare del trattamento deve fornire una spiegazione scritta ed è altresì invitato a notificare all'interessato, al titolare del trattamento delegato e, se del caso, al responsabile del trattamento, all'RPD e al DPB la sua decisione definitiva e le conclusioni del DPB. La decisione (costituita dal parere motivato del DPB e dalla decisione finale del titolare del trattamento) può essere impugnata dall'interessato chiedendo al Presidente dell'Ufficio di avviare la procedura di arbitrato prevista dall'articolo 52 DPR o dinanzi al tribunale amministrativo dell'Organizzazione internazionale del lavoro.

66. Conformemente alle linee guida dell'EDPB, ai criteri di riferimento per l'adeguatezza e alla giurisprudenza della CGUE, l'organo di controllo ha poteri vincolanti, in quanto ciò costituisce un fattore chiave per garantire l'efficacia del meccanismo di controllo.

---

(29) Decisione del Presidente dell'Ufficio sull'applicabilità delle raccomandazioni del responsabile della protezione dei dati approvate dal comitato per la protezione dei dati nel quadro delle conclusioni sugli audit e sulle ispezioni in materia di protezione dei dati, disponibile al seguente indirizzo https://link.epo.org/web/office/data-protection-and-privacy/en-decision-of-the-president-on-enforceability-of-dpo-conclusions-and-recommendations.pdf.

67. L'EDPB osserva che i pareri del DPB formulati nel contesto della gestione dei reclami rimangono non vincolanti. Mentre le conclusioni e le raccomandazioni dell'RPD - a seguito di indagini e audit che possono essere stati avviati su richiesta del DPB – possono diventare vincolanti dopo l'approvazione del DPB, non sembrano applicarsi ai casi avviati ai sensi dell'articolo 50 RGPD, ossia ai reclami degli interessati.

68. Alla luce di quanto sopra, l'EDPB invita la Commissione a verificare e garantire che i poteri del DPB siano vincolanti nel contesto della gestione dei reclami ai sensi dell'articolo 50 DPR, e a valutare se sia possibile prevedere ulteriori garanzie a tal fine.

69. Tuttavia, l'EDPB accoglie con favore il fatto che le decisioni del titolare del trattamento ai sensi dell'articolo 50, paragrafo 6, DPR possano essere impugnate, in quanto ciò fornisce agli interessati un meccanismo di ricorso necessario e consente l'applicazione della decisione dell'organo di controllo.

70. Inoltre, l'EDPB accoglie con favore il fatto che anche il DPB possa raccomandare la concessione di un risarcimento dei danni materiali o immateriali (articolo 50, paragrafo 3, DPR).

2.4.4 Meccanismi di ricorso e arbitrato

71. Secondo i criteri di riferimento per l'adeguatezza, gli interessati dovrebbero disporre di mezzi di ricorso efficaci, compreso il risarcimento dei danni derivanti dal trattamento illecito dei loro dati personali. Si tratta di un elemento fondamentale di un sistema di giudizio o arbitrato indipendente che consenta il pagamento di un indennizzo e l'imposizione di sanzioni, se del caso.

72. L'EDPB osserva che, secondo il quadro dell'OEB in materia di protezione dei dati, gli interessati hanno il diritto di richiedere un riesame del trattamento dei loro dati personali dinanzi ai titolari del trattamento delegati qualora ritengano che si sia verificata una violazione delle norme in materia di protezione dei dati. Ciò costituisce un prerequisito per la presentazione di un reclamo presso il DPB quale organo di controllo indipendente ai sensi dell'articolo 50 DPR. Tale requisito rappresenta una novità rispetto al sistema di protezione dei dati dell'UE, che tuttavia non compromette il livello di protezione offerto dal sistema dell'OEB, in quanto non influisce né sull'applicabilità dei diritti degli interessati né sul loro diritto al risarcimento.

73. Ai sensi dell'articolo 50 e dell'articolo 52, paragrafo 1, DPR, gli interessati che non sono soddisfatti della decisione finale adottata a seguito della procedura di cui all'articolo 50 DPR possono presentare ricorso. I dipendenti dell'OEB possono impugnare la decisione dinanzi al tribunale amministrativo dell'Organizzazione internazionale del lavoro. Qualsiasi altro interessato ha tre mesi di tempo per presentare al Presidente una richiesta di arbitrato.

74. L'EDPB accoglie con favore le disposizioni su un meccanismo di ricorso. Per quanto riguarda il meccanismo di arbitrato, l'EDPB osserva che è possibile prevedere meccanismi alternativi di risoluzione delle controversie, qualora non siano disponibili meccanismi giurisdizionali, ad esempio a causa dello status di organizzazione internazionale del titolare del trattamento. Tali meccanismi alternativi di risoluzione delle controversie devono offrire all'interessato garanzie sostanzialmente equivalenti a quelle richieste dall'articolo 47 della Carta ([30]). Pertanto, la previsione di un meccanismo alternativo non presenta di per sé alcuna preoccupazione né alcun problema ([31]), a condizione che l'arbitrato i) garantisca un giudizio indipendente e imparziale in conformità dei principi del giusto processo, ii) sia vincolante per il titolare del trattamento (OEB) ([32]), consenta iii) di ottenere un risarcimento e iv) di imporre sanzioni, ove opportuno.

75. Analogamente, la Corte europea dei diritti dell'uomo ha stabilito che è possibile fornire mezzi di ricorso efficaci attraverso «mezzi alternativi ragionevoli», come l'arbitrato ([33]).

76. L'EDPB rileva con soddisfazione che il quadro giuridico dell'OEB prevede i) norme per garantire l'indipendenza dell'arbitro (articolo 52, paragrafo 3, DPR), ii) la natura vincolante del meccanismo di arbitrato (articolo 52, paragrafo 1, DPR), nonché iii) il diritto al risarcimento dei danni subiti a causa di una violazione delle norme in materia di protezione dei dati (articolo 53 delle DPR) e iv) l'irrogazione di sanzioni, se del caso [articolo 11 del regolamento arbitrale della Corte europea di arbitrato ([34])].

77. Inoltre, l'EDPB accoglie con favore il fatto che i costi dell'arbitrato siano sostenuti dall'OEB, soddisfacendo in tal modo il requisito secondo cui i mezzi di ricorso per far rispettare i diritti degli interessati non devono comportare costi proibitivi ([35]).

([30]) CGUE, sentenza del 16 luglio 2020, causa C-311/18, *Data Protection Commissioner/Facebook Ireland Ltd e Maximillian Schrems* («Schrems II»), punti 96, 186 e segg.

([31]) Gruppo di lavoro Articolo 29 «Criteri di riferimento per l'adeguatezza», adottati il 28 novembre 2017, rivisti da ultimo e adottati il 6 febbraio 2018; linee guida 2/2020 sull'articolo 46, paragrafo 2, lettera a), e sull'articolo 46, paragrafo 3, lettera b), del regolamento (UE) 2016/679 per i trasferimenti di dati personali tra autorità e organismi pubblici del SEE ed extra-SEE, versione 2.0, adottata il 15 dicembre 2020, punti 53 e 75.

([32]) CGUE, sentenza del 6 ottobre 2015, causa C-362/14, *Maximillian Schrems/Data Protection Commissioner* («Schrems»), punti 41 e 95; CGUE, sentenza del 16 luglio 2020, causa C-311/18, *Data Protection Commissioner/Facebook Ireland Ltd e Maximillian Schrems* («Schrems II»), punti 186,187,189, 195 e segg.

([33]) Corte EDU, quinta sezione, decisione, domanda n. 415/07. *Roland KLAUSECKER/Germania*, disponibile al seguente indirizzo https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-151029%22.

([34]) Il regolamento arbitrale della Corte europea di arbitrato è disponibile al seguente indirizzo: https://cour-europe-arbitrage.org/arbitration-rules/

([35]) Gruppo di lavoro Articolo 29, WP 254 rev.01, adottato il 28 novembre 2017, rivisto da ultimo e adottato il 6 febbraio 2018, approvato dall'EDPB, paragrafo 4.

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

78. L'EDPB sottolinea, in via preliminare, che la valutazione dell'accesso ai dati personali trasferiti dall'Unione e il loro utilizzo da parte delle autorità pubbliche nel caso di specie è distinta dalla corrispondente valutazione del livello di protezione offerto da un paese terzo. Anziché valutare le leggi e le prassi pertinenti dei paesi terzi in materia di accesso da parte delle pubbliche amministrazioni, lo scenario specifico di una decisione di adeguata protezione dei dati personali da parte di un'organizzazione internazionale richiede il riesame delle norme che stabiliscono le modalità di trattamento, da parte tale organizzazione, delle richieste delle pubbliche amministrazioni di accesso ai dati personali, tra cui, in particolare, la possibilità di respingimento di tali richieste e le relative norme al riguardo. Pertanto, lo standard in base al quale viene valutata l'equivalenza essenziale differisce, per quanto riguarda l'accesso ai dati da parte delle pubbliche amministrazioni, dalle precedenti decisioni di adeguatezza.

79. Come ulteriore osservazione generale preliminare, l'EDPB rileva che, in base alle spiegazioni supplementari fornite dalla Commissione, l'OEB non ha ancora ricevuto alcuna richiesta di accesso ai dati a fini di applicazione della legge o di sicurezza nazionale.

80. Il fatto che finora presso l'OEB non siano state presentate richieste a fini di applicazione della legge o di sicurezza nazionale implica che le norme applicabili in tali casi non sono ancora state messe alla prova nella pratica. Pertanto, l'EDPB incoraggia la Commissione a monitorare se l'OEB riceverà richieste di questo tipo in futuro e le modalità di attuazione delle norme pertinenti nel contesto specifico. La Commissione potrebbe esaminare, in particolare, in che modo le norme e gli standard dell'OEB si applicano alle richieste delle forze dell'ordine e delle agenzie di intelligence, come ad esempio l'obbligo di fornire la prova che è necessario trasmettere i dati per una finalità specifica derivante dal dovere di cooperazione dell'OEB (articolo 8, paragrafo 3, DPR). Tale prova costituirà a sua volta la base per il riesame, da parte dell'OEB, della necessità e della proporzionalità di una trasmissione (articolo 8, paragrafo 4, DPR) ([36]).

3.1 Trattamento da parte dell'OEB delle richieste delle pubbliche amministrazioni di accesso ai dati personali

81. Il progetto di decisione sottolinea che il quadro giuridico nell'ambito del quale l'OEB valuta le richieste delle autorità pubbliche in merito ai dati personali e risponde ad esse deriva dai PPI, dalle prescrizioni delle DPR in materia di trasmissioni e trasferimenti di dati personali e dal diritto internazionale pubblico ([37]). Sebbene tale quadro si applichi in generale alle richieste provenienti sia da Stati contraenti che da Stati non contraenti, le disposizioni specifiche stabiliscono un regime diverso per le richieste provenienti da autorità pubbliche di Stati contraenti, da un lato, e di Stati non contraenti, dall'altro.

([36]) Per quanto riguarda il quadro giuridico per le trasmissioni, cfr. anche i precedenti punti 56 e 57 del presente parere.
([37]) Cfr. il considerando 96 del progetto di decisione.

82. Per quanto riguarda gli Stati contraenti, le immunità dell'OEB stabilite nei PPI (cfr. punto 14) sono integrate da un dovere di cooperazione. L'articolo 20, paragrafo 1, PPI stabilisce che l'OEB «*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*» ([38]). A tal fine, e come previsto dall'articolo 3, paragrafo 1, lettera a), PPI, l'OEB può rinunciare alla propria immunità di giurisdizione ed esecuzione per rispondere alle richieste di accesso delle pubbliche amministrazioni. L'EDPB osserva che appare infatti inevitabile prevedere meccanismi di cooperazione con le autorità pubbliche degli Stati contraenti, che in alcuni casi possono persino servire gli interessi dell'interessato, ad esempio per quanto riguarda le prestazioni sociali e le questioni assicurative del personale dell'OEB. Tuttavia, l'articolo 20, paragrafo 1, PPI solleva la questione, in particolare per quanto riguarda le richieste di accesso a fini di applicazione della legge e di sicurezza nazionale, del modo in cui il dovere di cooperazione si collega o interagisce con il concetto di immunità. La Commissione ha indicato che le norme dell'OEB sulla cooperazione devono essere intese come parte del più ampio principio generale di immunità, e pertanto l'OEB sarebbe in grado di respingere le richieste per le finalità di cui sopra, indipendentemente dall'articolo 20, paragrafo 1, PPI. L'EDPB invita la Commissione a chiarire ulteriormente questo punto nella decisione.

83. La decisione su una richiesta di cooperazione spetta al Presidente dell'Ufficio che, come indica il progetto di decisione, esercita un potere discrezionale in tal senso ([39]). Sebbene il progetto di decisione faccia riferimento all'articolo 3, paragrafo 1, lettera a), PPI come base giuridica per la rinuncia all'immunità dell'Organizzazione, esso non individua chiaramente una disposizione che attribuisce al Presidente il potere discrezionale di cui trattasi e che stabilisce i criteri che guidano l'esercizio di tale discrezionalità al momento di decidere in merito a una richiesta di cooperazione. L'EDPB osserva che, ai sensi dell'articolo 19, paragrafo 2, PPI, il Presidente «ha il dovere di revocare l'immunità quando ritiene che tale immunità impedisca il normale corso della giustizia e che sia possibile rinunciare a tale immunità senza compromettere gli interessi dell'Organizzazione». Tale requisito solleva ulteriori questioni sulla portata della discrezionalità del Presidente. Facendo seguito al paragrafo precedente, l'EDPB invita pertanto la Commissione a chiarire questi aspetti nella decisione.

84. Se l'OEB sceglie di soddisfare una richiesta di accesso di uno Stato contraente in linea con l'articolo 20, paragrafo 1, PPI, si applicano i requisiti delle DPR per le trasmissioni (cfr. paragrafi 38 e seguenti) ([40]). Tali norme sono applicabili a tutti gli Stati contraenti, indipendentemente dal fatto che lo Stato contraente sia uno Stato membro del SEE o si qualifichi come paese terzo dal punto di vista del diritto dell'UE in materia di protezione dei dati. Tuttavia, le norme per le trasmissioni, a differenza del regime per i trasferimenti alle autorità pubbliche al di fuori degli Stati contraenti dell'OEB, non richiedono esplicitamente che nel paese destinatario sia garantito un livello adeguato di protezione dei dati trasferiti ([41]). A tale riguardo, l'EDPB desidera ricordare le sue linee guida sull'articolo 48 del RGPD ([42]), che specificano che «*qualora i dati trattati nell'UE siano trasferiti o divulgati in risposta a una richiesta di un'autorità di un paese terzo, tale divulgazione è soggetta al RGPD e costituisce un trasferimento ai sensi del capo V. Ciò significa che, come per qualsiasi trasferimento soggetto al RGPD, devono*

([38]) In base alle informazioni supplementari fornite dalla Commissione, finora l'OEB non ha applicato l'autorità di cui all'articolo 20, paragrafo 2, e all'articolo 25 PPI per concludere accordi complementari con uno o più Stati contraenti a fini di applicazione della legge o di sicurezza nazionale.
([39]) Cfr. il considerando 97 del progetto di decisione.
([40]) Ibidem.
([41]) Cfr. i considerando da 63 a 65 del progetto di decisione e l'articolo 8 DPR.
([42]) Linee guida 2/2024 dell'EDPB sull'articolo 48 del RGPD, adottate il 2 dicembre 2024.

sussistere una base giuridica per il trattamento di cui all'articolo 6 e un motivo per il trasferimento di cui al capo V» ([43]). A tale riguardo, l'EDPB ribadisce la sua richiesta di chiarimenti di cui al precedente punto 41 e invita la Commissione a chiarire quali garanzie si applichino anche alle trasmissioni basate su richieste di accesso da parte delle pubbliche amministrazioni, in particolare richieste a fini di applicazione della legge e di sicurezza nazionale. Occorre garantire che i requisiti di cui al capo V del RGPD, nella misura necessaria a stabilire l'equivalenza essenziale, siano sufficientemente trattati, anche nei casi in cui il concetto di paesi terzi nella legislazione dell'UE in materia di protezione dei dati e nel quadro giuridico dell'OEB non coincidano pienamente ([44]).

85. Sebbene l'EDPB riconosca che la nota esplicativa dell'OEB sulla trasmissione e il trasferimento di dati personali afferma che «*per fornire garanzie adeguate come strumenti per le trasmissioni, negli strumenti applicabili, quali memorandum d'intesa o accordi amministrativi, dovrebbero essere inserite disposizioni specifiche in materia di protezione dei dati*» ([45]), potrebbe non essere fattibile, nella pratica, attuare tali strumenti nei confronti delle autorità di contrasto e delle agenzie di sicurezza nazionali. L'EDPB ritiene che le trasmissioni di dati personali a Stati membri contraenti ma non appartenenti al SEE, in particolare a fini di applicazione della legge e di sicurezza nazionale, richiederebbero pertanto una particolare attenzione da parte della Commissione.

86. Poiché non esiste uno strumento giuridico che disciplini specificamente il trattamento da parte dell'OEB delle richieste presentate da autorità pubbliche di Stati non contraenti, si applicano le norme generali per i trasferimenti ai sensi delle DPR, che sono molto simili a quelle del capo V del RGPD (cfr. paragrafi 35 e 36).

3.2 Limitazione dei diritti degli interessati

87. L'articolo 25 DPR prevede che specifiche disposizioni giuridiche del quadro giuridico dell'OEB possano limitare l'applicazione dei diritti dell'interessato, a condizioni molto simili a quelle previste dall'articolo 23 RGPD (cfr. paragrafi 33 e seguenti). Nel contesto dell'accesso delle pubbliche amministrazioni, l'EDPB osserva che la limitazione contenuta nella circolare n. 420, lettera h), può consentire un'interpretazione estensiva, in quanto fa ampio riferimento agli scenari di «*prestare o ricevere assistenza alle o dalle autorità pubbliche competenti, compresi gli Stati contraenti dell'OEB e le organizzazioni internazionali*». Pur riconoscendo che la portata di questa disposizione è limitata al personale dell'OEB, l'EDPB invita la Commissione a monitorarne l'applicazione pratica.

([43]) Ibidem, punto 9.
([44]) Pur riconoscendo che tutti gli Stati contraenti sono parti della CEDU e della Convenzione 108, l'EDPB ricorda che la ratifica di tali strumenti non può di per sé fornire un livello di protezione sostanzialmente equivalente, in quanto ciò dipenderà, in particolare, dalla loro specifica attuazione in ciascun paese.
([45]) EPO transmission and transfer of personal data, Explanatory Note (Trasmissione e trasferimento di dati personali da parte dell'OEB, nota esplicativa), versione del gennaio 2024, pag. 6.

4. ATTUAZIONE E MONITORAGGIO DEL PROGETTO DI DECISIONE

88. Per quanto riguarda il monitoraggio e il riesame della decisione di adeguatezza, l'EDPB osserva che, secondo la giurisprudenza della CGUE, «alla luce del fatto che il livello di protezione assicurato da un paese terzo [o da un'organizzazione internazionale] può evolversi, incombe alla Commissione, successivamente all'adozione di una decisione [di adeguatezza] in forza dell'articolo [45 del RGPD], verificare periodicamente se la constatazione relativa al livello di protezione adeguato assicurato dal paese terzo [o dall'organizzazione internazionale] in questione continui ad essere giustificata in fatto e in diritto. Una siffatta verifica è in ogni caso obbligatoria quando taluni indizi facciano sorgere un dubbio al riguardo» ([46]).

89. L'EDPB ritiene che la funzione di controllo – e in particolare l'esercizio dei poteri di indagine e correttivi – e l'accesso delle pubbliche amministrazioni ai dati trasferiti dall'UE all'OEB meriteranno un'attenzione specifica nel corso dei prossimi riesami periodici. Analogamente, durante il monitoraggio della decisione di adeguatezza, la Commissione dovrebbe prestare ulteriore attenzione all'evoluzione delle norme che integrano le DPR, come il documento «*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*» (Decisione del Presidente dell'Ufficio europeo dei brevetti del 12 luglio 2024 sull'applicabilità delle raccomandazioni del responsabile della protezione dei dati approvate dal comitato per la protezione dei dati nel quadro dei controlli e delle ispezioni in materia di protezione dei dati), il documento «*Data Protection Oversight - How the Data Protection Officer conducts DP Audits and DP Inspections*» (Controllo della protezione dei dati - Modalità di svolgimento degli audit e delle ispezioni in materia di protezione dei dati da parte del responsabile della protezione dei dati) e il documento «*EPO transmission and transfer of personal data, Explanatory Note»* (Trasmissione e trasferimento di dati personali da parte dell'OEB, nota esplicativa), versione del gennaio 2024.

90. L'EDPB osserva che il riesame della constatazione di adeguatezza avrà luogo almeno ogni quattro anni, conformemente all'articolo 45, paragrafo 3, RGPD.

91. Per quanto riguarda il coinvolgimento pratico dell'EDPB e dei suoi rappresentanti nella preparazione e nello svolgimento dei futuri riesami periodici, l'EDPB ribadisce che qualsiasi documentazione pertinente, compresa la corrispondenza, dovrebbe essere condivisa per iscritto con l'EDPB con sufficiente anticipo rispetto ai riesami.

92. L'EDPB accoglie con favore il fatto che il progetto di decisione preveda la partecipazione dell'EDPB alla riunione organizzata tra la Commissione e l'OEB e dedicata al riesame del funzionamento della decisione di adeguatezza.

Per il comitato europeo per la protezione dei dati

La presidente

(Anu Talus)

([46]) CGUE, sentenza del 6 ottobre 2015, causa C-362/14, *Maximillian Schrems/Data Protection Commissioner* («Schrems»), punto 76. Cfr. anche il considerando 105 e l'articolo 3, paragrafo 5, del progetto di decisione.