

**Parere 26/2025 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 del Regno Unito**

Adottato il 16 ottobre 2025

Sintesi

Il 22 luglio 2025 la Commissione europea ha avviato il processo di adozione del proprio progetto di decisione di esecuzione sull'adeguata protezione dei dati personali da parte del Regno Unito, a norma dell'articolo 45, paragrafo 2, del RGPD. Il presente progetto di decisione proroga la validità di alcune parti della precedente decisione sull'adeguatezza del 28 giugno 2021 a titolo di riferimento fino al dicembre 2031.

Lo stesso giorno la Commissione europea ha chiesto il parere del comitato europeo per la protezione dei dati («EDPB»). La valutazione dell'EDPB sull'adeguatezza del livello di protezione offerto dal Regno Unito 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 sia degli aspetti generali legati alla protezione dei dati del progetto di decisione sia dell'accesso da parte delle autorità pubbliche ai dati personali trasferiti dallo Spazio economico europeo (SEE) a fini di contrasto e di sicurezza nazionale, compresi i mezzi di ricorso a disposizione delle persone nel SEE.

L'EDPB ha inoltre valutato se le garanzie previste dal quadro giuridico del Regno Unito siano in atto ed efficaci.

Per tale lavoro l'EDPB si è basato principalmente sui criteri di riferimento per l'adeguatezza ai sensi del RGPD («criteri di riferimento per l'adeguatezza ai sensi del RGPD») adottati il 28 novembre 2017, rivisti da ultimo e adottati il 6 febbraio 2018, e sulle raccomandazioni 2/2020 dell'EDPB relative alle garanzie essenziali europee per le misure di sorveglianza.

L'EDPB accoglie con favore il continuo allineamento tra il quadro di protezione dei dati del Regno Unito e dell'UE, nonostante i recenti sviluppi nel pertinente quadro giuridico del Regno Unito. In tale contesto, il presente parere evidenzia diversi punti che richiedono un'ulteriore analisi, nonché alcune questioni che la Commissione dovrebbe monitorare attentamente nei prossimi anni nell'ambito del suo obbligo di monitoraggio ai sensi dell'articolo 45, paragrafo 4, del RGPD.

L'EDPB osserva che il Regno Unito ha introdotto modifiche per quanto riguarda il quadro giuridico generale dell'UE «ereditato» in virtù della legge del 2023 del Regno Unito sul diritto dell'UE conservato (revoca e riforma) («legge REUL») che, tra l'altro, elimina il principio del primato del diritto dell'Unione (con garanzie per alcune disposizioni del RGPD) ed elimina l'applicazione diretta dei principi del diritto dell'Unione, compreso il diritto alla vita privata e alla protezione dei dati sancito dalla Carta dei diritti fondamentali. L'EDPB invita la Commissione a spiegare e a effettuare una valutazione più dettagliata delle modifiche introdotte dalla legge REUL e a valutarne l'impatto sul quadro giuridico del Regno Unito in generale e più specificamente sul suo quadro in materia di protezione dei dati. L'EDPB ritiene inoltre che tale ambito debba essere oggetto di una stretta vigilanza da parte della Commissione in futuro.

L'EDPB osserva che al segretario di Stato sono stati conferiti nuovi poteri per introdurre modifiche al nuovo quadro in materia di protezione dei dati mediante regolamenti secondari, che richiedono un minore controllo parlamentare, in alcuni casi, ad esempio, i trasferimenti internazionali, il processo decisionale automatizzato e la governance della commissione per l'informazione. L'EDPB invita la Commissione a evidenziare nella decisione di adeguatezza finale gli ambiti che intende monitorare attentamente visto il rischio di ulteriori divergenze con il diritto dell'UE in materia di protezione dei dati in rapporto alla legislazione derivata del Regno Unito.

L'EDPB rileva modifiche alle norme che disciplinano il trasferimento di dati personali, in particolare il nuovo elenco indicativo di elementi da prendere in considerazione nella verifica dell'adeguatezza, che non include elementi importanti figuranti nella precedente verifica dell'adeguatezza del Regno Unito ⁽¹⁾. Ciò vale sia per i trasferimenti verso paesi terzi effettuati ai sensi del RGPD del Regno Unito sia per i trasferimenti di dati trattati a fini di contrasto. L'EDPB incoraggia la Commissione a sviluppare ulteriormente nello specifico la sua valutazione su tali aspetti e a monitorare gli sviluppi e l'attuazione pratica di questa nuova verifica dell'adeguatezza.

L'EDPB invita la Commissione a effettuare una valutazione più dettagliata della ristrutturazione dell'Information Commissioner's Office («ICO») in qualità di comitato nonché delle norme per la nomina e la revoca dei membri esecutivi e non esecutivi del comitato. L'EDPB invita inoltre la Commissione a fornire maggiori dettagli sulla recente consultazione dell'ICO, indetta dopo il presente progetto di decisione, al fine di introdurre un nuovo sistema di triage per la gestione dei reclami. L'EDPB invita la Commissione a monitorare tutti questi cambiamenti una volta entrati in vigore. Pur prendendo atto con soddisfazione della politica di trasparenza dell'ICO e della disponibilità dei dati statistici e analitici delle sue attività di applicazione delle norme, l'EDPB invita altresì la Commissione a effettuare una valutazione più dettagliata e a monitorare l'applicazione dei poteri correttivi, l'efficacia delle sanzioni e dei mezzi di ricorso per le parti interessate nel quadro del Regno Unito in materia di protezione dei dati.

L'EDPB ritiene essenziale valutare le esenzioni estese per motivi di sicurezza nazionale nell'ambito del quadro delle attività di contrasto e rimane particolarmente vigile per quanto riguarda eventuali deroghe al principio di proporzionalità nonché all'obbligo di trattare i dati personali per una finalità legittima. Analogamente, qualsiasi esenzione dai poteri dell'autorità di controllo dovrebbe essere affrontata con cautela. Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta devono rispettare il contenuto essenziale di detti diritti e libertà e, nel rispetto del principio di proporzionalità, possono essere apportate solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. L'EDPB invita la Commissione a integrare la sua valutazione nella decisione di adeguatezza finale e a monitorare nello specifico l'applicazione pratica delle esenzioni per motivi di sicurezza nazionale da parte delle autorità di contrasto.

L'EDPB osserva che le attività di trattamento svolte dalle autorità competenti per le attività di contrasto possono, in circostanze specifiche, rientrare nell'ambito di applicazione delle norme applicabili di consuetudine al trattamento dei dati personali da parte delle autorità di sicurezza nazionale. In siffatto contesto, particolare attenzione dovrebbe essere rivolta a garantire che il regime di protezione dei dati nell'ambito del trattamento a fini di sicurezza nazionale non sia esteso a contesti non correlati a quelli nazionali. L'EDPB invita la Commissione a monitorare se le autorità competenti qualificate siano in grado di mantenere una chiara distinzione tra le diverse finalità di trattamento al fine di rispettare di conseguenza il corrispondente quadro giuridico.

L'EDPB accoglie con favore i chiarimenti occorsi tra il Regno Unito e gli Stati Uniti nel contesto dell'accordo tra Regno Unito e Stati Uniti sulla legge CLOUD, che apportano una maggiore precisazione sul piano giuridico. Allo stesso tempo, l'EDPB desidera ricordare la necessità di migliorare il livello di garanzie previste dall'accordo quadro UE-USA, le cui garanzie in materia di protezione della vita privata

⁽¹⁾ i) le norme del paese terzo in materia di sicurezza pubblica, difesa, sicurezza nazionale e diritto penale e accesso ai dati personali da parte delle autorità pubbliche, ii) la giurisprudenza, iii) l'esistenza di diritti effettivi e azionabili di cui godono gli interessati e i mezzi di ricorso amministrativi e giurisdizionali che gli interessati i cui dati personali sono trasferiti possono effettivamente proporre, e iv) una o più autorità di controllo indipendenti.

e dei dati sono integrate nell'accordo tra Regno Unito e Stati Uniti sulla legge CLOUD. Nel complesso, l'EDPB ritiene necessario chiarire la valutazione della Commissione relativa all'accordo tra Regno Unito e Stati Uniti sulla legge CLOUD e qualsiasi eventuale ripercussione sul livello di protezione. L'EDPB invita la Commissione a continuare a includere l'accordo tra Regno Unito e Stati Uniti sulla legge CLOUD nelle sue valutazioni e riesami futuri.

Come recentemente sottolineato nella dichiarazione 05/2024, l'EDPB ritiene che la cifratura sia essenziale per garantire la sicurezza e la riservatezza dei dati personali e delle comunicazioni elettroniche. Le comunicazioni relative alle capacità tecniche ai sensi della legge del 2016 sui poteri di indagine (Investigatory Powers Act 2016, «IPA 2016»), che obbligano le imprese a dare la possibilità di rimuovere la cifratura su richiesta del governo, creano vulnerabilità sistemiche e rappresentano una minaccia diretta all'integrità e alla riservatezza delle comunicazioni elettroniche. Tali sviluppi meritano attenzione nella decisione sull'adeguatezza, in particolare alla luce dell'articolo 45, paragrafo 2, lettera a), del RGPD, che richiede una valutazione non solo del quadro giuridico sulla carta, ma anche della sua attuazione, e dovrebbe essere monitorata.

L'EDPB osserva che la legge di modifica del 2024 sui poteri d'indagine (Investigatory Powers Amendment Act 2024, «IPAA 2024») ha introdotto un regime specifico per la conservazione e l'esame di serie massive di dati personali in relazione alle quali le persone cui si riferiscono i dati personali non potrebbero avere solo una scarsa o nessuna ragionevole aspettativa di tutela della vita privata. L'EDPB ritiene necessari ulteriori chiarimenti per quanto riguarda le modifiche pertinenti, in particolare per quanto concerne i concetti di «autorizzazioni individuali» e «autorizzazioni per categoria». Inoltre, l'EDPB invita la Commissione a monitorare attentamente l'attuazione nella pratica dell'espressione «scarsa o nessuna ragionevole aspettativa di tutela della vita privata».

Indice

1. INTRODUZIONE.....	7
1.1. Ambito di applicazione del progetto di decisione della Commissione	7
1.2. Ambito di applicazione del presente parere dell'EDPB.....	8
1.3. Sviluppi NEL quadro giuridico del Regno Unito.....	9
1.4. Osservazioni di carattere generale e problematiche	10
1.4.1. Impegni internazionali assunti dal Regno Unito	10
1.4.2. Poteri del segretario di Stato di introdurre modifiche alla DUAA mediante regolamentazione secondaria	11
2. Aspetti generali relativi alla protezione dei dati	11
2.1. Interessi legittimi riconosciuti	11
2.1.1. Osservazioni generali	11
2.1.2. Divulgazione ai fini del trattamento di cui all'articolo 6, paragrafo 1, lettera e)	12
2.2. Diritti delle persone fisiche	13
2.2.1. Diritti di accesso	13
2.2.2. Garanzie per l'«esenzione per motivi di immigrazione».....	14
2.3. Limitazioni ai trasferimenti successivi.....	15
2.4. Processo decisionale automatizzato	16
2.4.1. Processo decisionale automatizzato e coinvolgimento umano	17
3. Meccanismo di procedura e applicazione.....	18
3.1. Vigilanza e applicazione.....	18
3.1.1. Vigilanza indipendente.....	18
3.1.2. Applicazione, comprese le sanzioni.....	19
4. DATI PERSONALI: ACCESSO E UTILIZZO SE TRASFERITI DA AUTORITÀ PUBBLICHE DALL'UNIONE EUROPEA AL REGNO UNITO	21
4.1. Accesso e uso da parte delle autorità pubbliche del Regno Unito a fini di contrasto penale ..	21
4.1.1. Basi giuridiche e garanzie applicabili.....	21
4.1.1.1. Poteri di indagine a fini di contrasto	21
4.1.1.2. Esenzioni per motivi di sicurezza nazionale per le autorità di contrasto.....	22
4.1.2. Controlli congiunti tra le agenzie di intelligence del Regno Unito e le autorità di contrasto	24
4.1.3. Il diritto di accesso.....	25
4.1.4. Trasferimenti successivi	25
4.1.4.1. Una nuova verifica della protezione dei dati.....	25

4.1.4.2.	Accordo tra Regno Unito e Stati Uniti sulla legge CLOUD	26
4.1.5.	Vigilanza e ricorso.....	28
4.2.	Accesso e uso da parte delle autorità pubbliche del Regno Unito a fini di sicurezza nazionale	29
4.2.1.	Utilizzo degli avvisi di capacità tecniche.....	29
4.2.2.	Basi giuridiche e garanzie applicabili.....	30
4.2.3.	Vigilanza e ricorso.....	32
5.	Riesame, durata e rinnovo del progetto di decisione	32

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: il «RGPD»),

visto l'accordo sullo Spazio economico europeo (SEE), in particolare l'allegato XI e il protocollo 37 dello stesso, modificato dalla decisione n. 154/2018 del comitato misto SEE, del 6 luglio 2018 ⁽²⁾,

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

HA ADOTTATO IL SEGUENTE PARERE:

1. INTRODUZIONE

1.1. AMBITO DI APPLICAZIONE DEL PROGETTO DI DECISIONE DELLA COMMISSIONE

1. Il 22 luglio 2025 la Commissione europea («Commissione») ha chiesto il parere del comitato europeo per la protezione dei dati («EDPB») sul progetto di decisione di esecuzione che modifica la decisione di esecuzione (UE) 2021/1772 della Commissione, del 28 giugno 2021, a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte del Regno Unito («progetto di decisione»). Nel suo progetto di decisione, la Commissione ha concluso che il Regno Unito continua a garantire un livello adeguato di protezione dei dati personali trasferiti dall'Unione europea nel Regno Unito nell'ambito di applicazione del RGPD.
2. L'EDPB osserva che il presente progetto di decisione proroga di sei anni la validità della decisione di esecuzione (UE) 2021/1772 della Commissione, del 28 giugno 2021, a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte del Regno Unito («precedente decisione di adeguatezza del Regno Unito»), che doveva scadere il 27 giugno 2025 (clausola di temporaneità). La precedente decisione di adeguatezza del Regno Unito era stata prorogata di sei mesi, fino al 27 dicembre 2025 in virtù della decisione (UE) 2025/1225 del 24 giugno 2025, per consentire al Regno Unito di portare a termine le riforme in materia di protezione dei dati ⁽³⁾.
3. Nel suo progetto di decisione, la Commissione ha valutato se la conclusione secondo cui il Regno Unito assicura un livello di protezione adeguato rimanga giustificata sotto il profilo fattuale e giuridico alla luce degli sviluppi intervenuti dopo l'adozione della precedente decisione di adeguatezza del Regno Unito.
4. La Commissione ha concentrato la sua valutazione sui nuovi sviluppi della legislazione del Regno Unito in materia di protezione dei dati, in particolare quelli introdotti dalla legge del 2025 sui dati in termini di uso e accesso («la DUAA»). La Commissione ha esaminato nello specifico gli elementi elencati nel

⁽²⁾ Nel presente parere, con il termine «Stati membri» si intendono gli «Stati membri del SEE».

⁽³⁾ Su richiesta, l'EDPB ha emesso il parere 06/2025 sulla proroga delle decisioni di esecuzione della Commissione europea a norma del RGPD e della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie sull'adeguata protezione dei dati personali nel Regno Unito.

considerando 281 della precedente decisione sull'adeguatezza del Regno Unito, che figurano tutti nel progetto di decisione.

5. L'EDPB concorda sul fatto che la valutazione dovrebbe concentrarsi principalmente su tutti i nuovi sviluppi pertinenti nella legislazione del Regno Unito e sugli elementi evidenziati nella precedente decisione di adeguatezza del Regno Unito nella misura in cui sono valutati tutti gli elementi di cui all'articolo 45, paragrafo 2, del RGPD. L'EDPB accoglierebbe quindi con favore l'eventualità che, nella sua decisione di adeguatezza finale, la Commissione chiarisca esplicitamente che tutti gli elementi elencati nell'articolo 45, paragrafo 2, del RGPD, siano stati valutati al fine di concludere che il quadro giuridico generale del Regno Unito continua a garantire un livello adeguato di protezione dei dati personali trasferiti dall'Unione europea al Regno Unito. L'EDPB accoglierebbe inoltre con favore un chiarimento da parte della Commissione, la quale dichiara di valutare tali elementi in maniera continuativa nell'ambito del proprio ruolo di monitoraggio.

1.2. AMBITO DI APPLICAZIONE DEL PRESENTE PARERE DELL'EDPB

6. L'EDPB dovrebbe fornire alla Commissione un parere indipendente per la valutazione dell'adeguatezza del livello di protezione in un paese terzo ⁽⁴⁾, individuare eventuali carenze del quadro di adeguatezza e adoperarsi per formulare proposte per affrontarle ⁽⁵⁾. Data la situazione specifica del Regno Unito, la nuova decisione sull'adeguatezza integra la decisione sull'adeguatezza del 2021, che rimane valida per le parti non specificamente trattate nel presente progetto di decisione. Analogamente con il presente parere, l'EDPB si basa sul parere 14/2021 e lo sviluppa ulteriormente ⁽⁶⁾. Di conseguenza, l'analisi e le osservazioni dell'EDPB fornite nel suo precedente parere in merito alla precedente decisione di adeguatezza del Regno Unito restano generalmente pertinenti.
7. Alla luce di quanto precede, l'EDPB ha concentrato le proprie osservazioni su punti selezionati presentati nel progetto di decisione, in particolare quando sono necessari ulteriori chiarimenti, informazioni supplementari o un futuro monitoraggio da parte della Commissione europea.
8. L'EDPB osserva inoltre che, ai sensi degli articoli 47 e 94 del regolamento (UE) 2018/1725 ⁽⁷⁾, le istituzioni, gli organi e gli organismi dell'Unione europea possono trasferire dati personali verso un paese terzo, un territorio, un settore o un'organizzazione internazionale riconosciuti dalla Commissione europea a norma dell'articolo 45, paragrafo 3, del RGPD, in quanto garantisce un livello di protezione adeguato, a condizione che il trasferimento sia funzionale esclusivamente a compiti di competenza del titolare del trattamento, senza richiedere ulteriori autorizzazioni. L'EDPB invita la Commissione a ricordare questa possibilità giuridica nei considerando della decisione di adeguatezza finale.

⁽⁴⁾ Cfr. l'articolo 70, paragrafo 1, lettera s), del RGPD.

⁽⁵⁾ Cfr. gruppo di lavoro «Articolo 29», criteri di riferimento per l'adeguatezza, capitolo 2: aspetti procedurali per i riscontri relativi all'adeguatezza a norma del regolamento, adottati il 28 novembre 2017, versione emendata e adottata il 6 febbraio 2018, WP254 rev.01 (approvato dall'EDPB, cfr. <https://edpb.europa.eu/our-worktools/general-guidance/endorsed-wp29-guidelines>); (in appresso «criteri di riferimento per l'adeguatezza ai sensi del RGPD»).

⁽⁶⁾ Parere 14/2021 relativo al progetto di decisione di esecuzione della Commissione europea a norma del regolamento (UE) 2016/679 sull'adeguata protezione dei dati personali nel Regno Unito, adottato il 13 aprile 2021, https://www.edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf.

⁽⁷⁾ 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).

1.3. SVILUPPI NEL QUADRO GIURIDICO DEL REGNO UNITO

9. Come chiarito nel progetto di decisione ⁽⁸⁾, dopo la fine del periodo di attuazione concordato nell'accordo di recesso tra il Regno Unito e l'UE ⁽⁹⁾ il 31 dicembre 2020, il Regno Unito aveva intenzione di adottare un nuovo regime di protezione dei dati che si discostava dal quadro giuridico dell'UE. Infine, il Regno Unito ha apportato modifiche limitate al proprio quadro vigente in materia di protezione dei dati, in particolare in virtù della DUAA.
10. Al di là della protezione dei dati, una delle modifiche più importanti apportate al quadro giuridico del Regno Unito, dall'adozione della precedente decisione di adeguatezza del Regno Unito, riguarda il quadro giuridico generale «ereditato» dall'UE (denominato «diritto dell'UE conservato»), ossia le disposizioni giuridiche integrate nel diritto del Regno Unito mediante la legge dell'Unione europea (recesso) del 2018. Il diritto dell'UE conservato comprendeva i principi generali del diritto dell'UE, tra cui i diritti fondamentali derivanti dalla Carta dei diritti fondamentali dell'Unione europea («la Carta») ⁽¹⁰⁾ e i principi di proporzionalità e necessità, che hanno avuto un ruolo determinante nello sviluppo e nell'interpretazione della normativa sulla protezione dei dati nel Regno Unito. Ai sensi della legge dell'Unione europea (recesso) del 2018, il diritto dell'UE conservato aveva mantenuto il suo status di supremazia sul diritto derivato del Regno Unito e il diritto dell'UE mantenuto doveva essere interpretato in linea con i principi generali del diritto dell'UE. Tuttavia, dall'introduzione della legge sul diritto dell'UE mantenuto (revoca e riforma) del 2023 («legge REUL») ⁽¹¹⁾, il Regno Unito ha eliminato l'applicazione diretta dei principi del diritto dell'UE dal suo diritto nazionale, compresi i diritti fondamentali derivanti dalla Carta. La legge REUL ha inoltre abolito il principio della supremazia del diritto dell'Unione, in quanto il diritto dell'Unione conservato (ora denominato «diritto consuetudinario») deve essere letto in modo compatibile con il diritto nazionale del Regno Unito e non in linea con i principi del diritto dell'UE. Ciò costituisce un cambiamento significativo nell'ordinamento giuridico del Regno Unito.
11. Inoltre, sebbene attualmente in sospeso, grazie alla legge REUL ⁽¹²⁾ potrebbe essere introdotto un nuovo criterio giuridico più flessibile che consenta ai giudici della Corte d'appello e della Corte suprema di discostarsi dalla giurisprudenza dell'UE conservata. Tale modifica, se adottata, potrebbe costituire un cambiamento significativo nel Regno Unito.
12. Nonostante tali modifiche, l'EDPB esprime apprezzamento per l'inclusione di garanzie nella legge REUL per garantire che, in determinate circostanze, la legislazione in materia di protezione dei dati non sia superata. Tali garanzie comprendono i requisiti secondo cui qualsiasi atto legislativo che imponga l'obbligo o conferisca il potere di trattare i dati personali non prevalga su un requisito previsto dalla principale normativa sulla protezione dei dati relativo al trattamento di dati personali e che il quadro relativo alla protezione dei dati continui a prevalere su altre normative del Regno Unito ⁽¹³⁾. Tuttavia, l'EDPB osserva che tali garanzie comprendono anche due eccezioni: i) quella in cui il parlamento del Regno Unito può scegliere di derogare deliberatamente ai requisiti in materia di protezione dei dati ⁽¹⁴⁾

⁽⁸⁾ Cfr. il considerando 2 del progetto di decisione.

⁽⁹⁾ Il periodo di attuazione è un periodo di tempo concordato nell'accordo di recesso Regno Unito-UE in cui il Regno Unito cessa di essere membro dell'UE, ma continuerà a essere soggetto alle norme dell'UE e a far parte del mercato unico e dell'unione doganale. Cfr. la legge del 2020 sul recesso dall'Unione europea (accordo di recesso).

⁽¹⁰⁾ Carta dei diritti fondamentali dell'Unione europea (GU C 326 del 26.10.2012, pagg. 391-407).

⁽¹¹⁾ Cfr. il considerando 11 del progetto di decisione.

⁽¹²⁾ Cfr. l'articolo 6 della Retained EU Law (Revocation and Reform) Act 2023 (Commencement No. 2 and Saving Provisions) (Revocation) Regulations 2024.

⁽¹³⁾ Cfr. l'articolo 183 A della DPA 2018, introdotto dall'articolo 106, paragrafo 2, della DUAA.

⁽¹⁴⁾ Cfr. articolo 183 A, paragrafo 3, DPA 2018, introdotto dall'articolo 106, paragrafo 2, della DUAA.

e ii) quella in cui talune disposizioni della legge del 2018 sulla protezione dei dati (Data Protection Act 2018, «DPA 2018») sono esenti e, in quanto tali, prevarranno sul RGPD del Regno Unito ⁽¹⁵⁾. Le implicazioni della seconda esenzione sono ancora incerte e dibattute nel Regno Unito.

13. Per quanto riguarda la tutela dei diritti fondamentali sanciti dalla Carta, il considerando 12 del progetto di decisione spiega che qualsiasi riferimento ai diritti e alle libertà fondamentali nel RGPD del Regno Unito e nel DPA 2018 è stato sostituito da riferimenti ai diritti ai sensi della Convenzione europea dei diritti dell'uomo, integrati nella legislazione nazionale ai sensi della legge sui diritti umani del 1998 ⁽¹⁶⁾.
14. L'EDPB invita la Commissione a effettuare una valutazione più dettagliata di tali modifiche all'ordinamento giuridico del Regno Unito di cui ai precedenti punti 10, 11 e 12, al fine di spiegare le modifiche apportate dalla legge REUL e valutarne l'impatto sul quadro giuridico britannico in materia di protezione dei dati. L'EDPB ritiene inoltre che questo sia un settore da monitorare attentamente in futuro da parte della Commissione e invita la Commissione a farlo.
15. Infine, l'EDPB prende atto di diverse modifiche nell'ambito della DUA sul quadro giuridico applicabile alle comunicazioni elettroniche, compresi i cookie, e ricorda che il trattamento dei dati personali potrebbe essere soggetto al campo di applicazione materiale del RGPD del Regno Unito ⁽¹⁷⁾. Invita pertanto la Commissione a includerli nella sua valutazione per la decisione finale nella misura in cui potrebbero avere un impatto sulla protezione dei dati. L'EDPB invita inoltre la Commissione a monitorare attentamente l'effetto pratico delle modifiche relative ai cookie esenti dal consenso.

1.4. OSSERVAZIONI DI CARATTERE GENERALE E PROBLEMATICHE

1.4.1. IMPEGNI INTERNAZIONALI ASSUNTI DAL REGNO UNITO

16. Per quanto riguarda gli impegni internazionali assunti dal Regno Unito ⁽¹⁸⁾, l'EDPB accoglie con favore il fatto che il Regno Unito continui a rispettare la CEDU e a essere soggetto alla giurisdizione della Corte europea dei diritti dell'uomo. Il Regno Unito ha inoltre aderito alla convenzione 108 ⁽¹⁹⁾ e al relativo protocollo addizionale ⁽²⁰⁾ e ha firmato la convenzione 108+ ⁽²¹⁾ nel 2018. Questi impegni internazionali sono elementi importanti ⁽²²⁾ e dovrebbero essere presi in considerazione nell'ambito della valutazione per il rinnovo di entrambe le decisioni sull'adeguatezza del Regno Unito ai sensi del RGPD e della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie.

⁽¹⁵⁾ Tali disposizioni sono elencate all'articolo 186, paragrafo 3, del DPA 2018. Ciò significa che, in caso di conflitto tra l'articolo 23 del RGPD del Regno Unito e una delle parti elencate, ad esempio l'allegato 2 del DPA 2018, contenente le esenzioni ai diritti degli interessati, prevarrà l'interpretazione della DPA 2018.

⁽¹⁶⁾ Cfr. l'articolo 8 della Convenzione europea dei diritti dell'uomo.

⁽¹⁷⁾ EDPB, parere 5/2019 sull'interazione tra la direttiva e-privacy e il regolamento generale sulla protezione dei dati, in particolare per quanto concerne competenze, compiti e poteri delle autorità per la protezione dei dati adottato il 12 marzo 2019, https://www.edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf.

⁽¹⁸⁾ Cfr. il capitolo 1: alcune informazioni di ampia portata relative al concetto di adeguatezza dei criteri di riferimento per l'adeguatezza.

⁽¹⁹⁾ Cfr. la convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale («convenzione 108») del 28 gennaio 1981.

⁽²⁰⁾ Cfr. il protocollo addizionale alla convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, concernente le autorità di controllo e i flussi transfrontalieri di dati, aperto alla firma l'8 novembre 2001.

⁽²¹⁾ Cfr. il protocollo che modifica la convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale (convenzione 108+) del 18 maggio 2018.

⁽²²⁾ Cfr. il considerando 105 del RGPD.

17. Nel complesso, l'EDPB sostiene gli sforzi volti a una rapida ratifica della convenzione 108+ da parte di paesi terzi come passo significativo verso l'allineamento ai principi riconosciuti a livello internazionale in materia di protezione dei dati e come segnale del loro impegno rispetto a norme e diritti fondamentali più ampi.

1.4.2. POTERI DEL SEGRETARIO DI STATO DI INTRODURRE MODIFICHE ALLA DUAA MEDIANTE REGOLAMENTAZIONE SECONDARIA

18. Sebbene la maggior parte delle modifiche introdotte al quadro di protezione dei dati del Regno Unito miri a chiarire e favorire il rispetto della legge, alcune possono ripercuotersi, a seconda della loro attuazione, sul livello di protezione dei dati personali nel Regno Unito.
19. A tale riguardo, l'EDPB osserva che al segretario di Stato sono stati conferiti nuovi poteri per introdurre modifiche alla DUAA mediante regolamentazione secondaria, che richiede un minor controllo parlamentare. In alcuni casi, ad esempio, i trasferimenti internazionali (cfr. l'articolo 2.3), il processo decisionale automatizzato (cfr. l'articolo 2.4.) e la governance dell'Information Commissioner (cfr. l'articolo 3), questi nuovi poteri sono ampi e il progetto di decisione non fornisce ulteriori informazioni sulle garanzie che saranno messe in atto e sul modo in cui tali poteri saranno utilizzati nella pratica.
20. L'EDPB invita la Commissione a evidenziare nella decisione di adeguatezza finale gli ambiti che intende monitorare attentamente visto il rischio di ulteriori divergenze con il diritto dell'UE in materia di protezione dei dati in rapporto alla legislazione derivata del Regno Unito.

2. ASPETTI GENERALI RELATIVI ALLA PROTEZIONE DEI DATI

2.1. INTERESSI LEGITTIMI RICONOSCIUTI

2.1.1. OSSERVAZIONI GENERALI

21. Nei considerando 22, 23 e 24, la Commissione concentra la sua valutazione sull'introduzione di una nuova base giuridica, ossia il trattamento necessario ai fini di un interesse legittimo riconosciuto. L'allegato 1 del RGPD del Regno Unito aggiornato elenca tali interessi legittimi riconosciuti.
22. Secondo gli orientamenti dell'ICO in materia ⁽²³⁾, i titolari del trattamento che fanno affidamento su un interesse legittimo riconosciuto come base giuridica sono comunque tenuti a rispettare tutti gli altri requisiti previsti dal RGPD del Regno Unito, ivi compresa la garanzia che il trattamento sia necessario e proporzionato per conseguire la finalità preventivamente approvata. Poiché tale aspetto non viene ricordato nel progetto di decisione e costituisce un elemento essenziale per concludere che la nuova base giuridica non compromette il livello di protezione dei diritti degli interessati, l'EDPB invita la Commissione a chiarire tale punto.
23. L'elencazione dei interessi legittimi riconosciuti nella legge non sembra di per sé porre problemi, tantomeno la decisione di introdurre tale nuova base giuridica – che apporta una maggiore chiarezza ai titolari del trattamento e dovrebbe essere accolta con favore.

⁽²³⁾ Cfr. gli orientamenti dell'ICO sui legittimi interessi, disponibili all'indirizzo <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/>.

24. Tuttavia, l'EDPB prende atto del fatto che alcuni interessi legittimi riconosciuti consistono in quanto segue: i) la necessità di trattare i dati personali per salvaguardare la sicurezza nazionale, proteggere la sicurezza pubblica o per motivi di difesa («condizione di sicurezza nazionale, sicurezza pubblica e difesa»); ii) la necessità di trattare i dati personali per individuare, investigare o prevenire un reato («condizione di reato»); e iii) la «divulgazione ai fini del trattamento di cui all'articolo 6, paragrafo 1, lettera e)».
25. Per quanto riguarda la «condizione di sicurezza nazionale, sicurezza pubblica e difesa» e la «condizione di reato», l'EDPB osserva che nel progetto di decisione non sono state incluse ulteriori informazioni sull'uso pratico di queste basi giuridiche da parte dei titolari e dei responsabili del trattamento. L'EDPB gradirebbe che la Commissione fornisse ulteriori dettagli sulle ulteriori informazioni e garanzie ricevute dalle autorità competenti del Regno Unito in merito all'applicazione pratica di tale base giuridica e invita la Commissione a monitorarne l'applicazione.
26. L'EDPB osserva inoltre che l'ICO sta lavorando a orientamenti specifici in materia, che, al momento del presente parere, comprendono una definizione di tali concetti. Data l'importanza dei chiarimenti su questi concetti, l'EDPB invita la Commissione a monitorare attentamente l'elaborazione degli orientamenti dell'ICO.

2.1.2. DIVULGAZIONE AI FINI DEL TRATTAMENTO DI CUI ALL'ARTICOLO 6, PARAGRAFO 1, LETTERA E)

27. L'EDPB osserva che l'interesse legittimo riconosciuto di recente istituzione che consente la «divulgazione ai fini del trattamento di cui all'articolo 6, paragrafo 1, lettera e)» introduce la possibilità di condividere i dati personali con le autorità pubbliche su base volontaria. Come chiarito dall'ICO nei suoi recenti orientamenti ⁽²⁴⁾, questo interesse legittimo riconosciuto non conferisce di per sé alle autorità richiedenti il diritto di accesso ai dati personali, ma un titolare del trattamento può invocare tale interesse approvato preventivamente qualora le autorità indichino che esse richiedono i dati per l'espletamento delle loro funzioni o compiti istituzionali. L'EDPB osserva inoltre che tali richieste di divulgazione per l'espletamento di compiti istituzionali non solo possono essere emesse per dati personali destinati a essere utilizzati per le finalità disciplinate dal RGPD del Regno Unito, ma possono anche riguardare le finalità del trattamento di cui alle parti 3 e 4 della legge sulla protezione dei dati del 2018. Di conseguenza, la modifica è pertinente anche per quanto concerne l'accesso da parte di pubbliche amministrazioni a fini di contrasto e di sicurezza nazionale ⁽²⁵⁾.
28. In tale contesto, si pone la questione di quali criteri il titolare del trattamento debba valutare per decidere se fornire volontariamente dati in risposta a una richiesta di informazioni. In particolare, come sottolineato dall'ICO nei suoi orientamenti ⁽²⁶⁾, l'EDPB comprende che il criterio di necessità per questa condizione di interesse legittimo riconosciuto è diversa dalle altre condizioni specificate nell'allegato 1. Riguardo alle richieste di divulgazione per l'espletamento di compiti istituzionali, per necessità si intende che il titolare del trattamento deve esaminare quale trattamento è necessario per divulgare le informazioni personali richieste. Il titolare del trattamento deve valutare se le informazioni che desiderano condividere sono proporzionate e necessarie per accogliere la richiesta. Per contro, il criterio della necessità non si estende alla questione se i dati personali siano effettivamente necessari

⁽²⁴⁾ Cfr. la nota 23.

⁽²⁵⁾ Cfr. gli orientamenti dell'ICO sulla condizione della richiesta di divulgazione per l'espletamento di compiti istituzionali, disponibili all'indirizzo <https://ico.org.uk/for-organisations/recognised-legitimate-interest-guidance/what-are-the-recognised-legitimate-interest-conditions/public-task-disclosure-request-condition/>.

⁽²⁶⁾ Cfr. la nota 23.

per espletare il compito o la funzione istituzionale, in quanto il titolare del trattamento può basarsi sulla dichiarazione del richiedente secondo cui ha bisogno delle informazioni personali per un determinato compito istituzionale ⁽²⁷⁾. Di fatto, in molti casi, in particolare quando le richieste sono presentate a fini di contrasto o di sicurezza nazionale, il titolare del trattamento non sarà in grado di effettuare tale valutazione.

29. In tale contesto, l'EDPB invita la Commissione a monitorare attentamente l'applicazione pratica di questa disposizione.
30. A parere dell'EDPB, le autorità di contrasto e quelle preposte alla sicurezza nazionale non dovrebbero utilizzare questo meccanismo per eludere le restrizioni giuridiche esistenti in merito ai loro poteri vincolanti di raccolta dei dati o per ottenere un numero di dati superiore a quello strettamente necessario per l'adempimento dei loro compiti. Inoltre, l'EDPB ritiene importante che i titolari del trattamento tengano conto degli orientamenti dell'ICO su come convalidare una richiesta di divulgazione per l'espletamento di compiti istituzionali e invita la Commissione a includere questo aspetto nel riesame periodico della decisione ⁽²⁸⁾.

2.2. DIRITTI DELLE PERSONE FISICHE

31. L'EDPB prende atto dell'analisi della Commissione secondo cui vi sono state modifiche limitate nel settore dei diritti delle persone fisiche. Ciò include modifiche all'articolo 12 e un nuovo articolo 12 A del RGPD del Regno Unito, che specifica ulteriormente i termini per rispondere alle richieste degli interessati ⁽²⁹⁾. Inoltre, l'articolo 13, paragrafo 5, del RGPD del Regno Unito prevede un'esenzione al diritto di informazione se i dati personali sono trattati a fini di ricerca scientifica o storica conformemente alle ulteriori garanzie di cui all'articolo 84 B del RGPD del Regno Unito. L'EDPB ritiene che entrambe le modifiche non compromettano il livello di protezione sostanzialmente equivalente fornito dal RGPD del Regno Unito.

2.2.1. DIRITTI DI ACCESSO

32. L'articolo 15, paragrafo 1 A, del RGPD del Regno Unito introduce una valutazione della proporzionalità, sviluppata ai sensi della giurisprudenza nazionale del Regno Unito. In particolare, i titolari del trattamento devono solo effettuare «ricerche ragionevoli e proporzionate» per soddisfare le richieste di accesso.
33. L'EDPB osserva che tale valutazione della proporzionalità non è presente nel quadro dell'UE in materia di protezione dei dati, che non prevede alcuna riserva generale alla proporzionalità per quanto riguarda gli sforzi che il titolare del trattamento deve intraprendere per soddisfare la richiesta degli interessati ai sensi dell'articolo 12 del RGPD, ma prevede solo motivi di rifiuto nella sottosezione 5 ⁽³⁰⁾.

⁽²⁷⁾ Cfr. la nota 23.

⁽²⁸⁾ Nei suoi orientamenti sulla condizione della richiesta di divulgazione per l'espletamento di compiti istituzionali (cfr. la nota 25), l'ICO chiarisce che i titolari del trattamento dovrebbero, ad esempio, chiedere che la richiesta sia formulata per iscritto ed effettuare controlli per garantire l'autenticità della richiesta o l'autorità del dipendente ad agire per l'organizzazione in cui lavora.

⁽²⁹⁾ In particolare a causa della necessità di confermare l'identità di un interessato o del pagamento di una tassa.

⁽³⁰⁾ Articolo 12, paragrafo 5: «Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 22 e dell'articolo 34 sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può: a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o

34. Pertanto, a parere dell'EDPB, è importante definire adeguatamente il concetto di «ricerche ragionevoli e proporzionate», che dovrebbe essere interpretato in modo restrittivo e sufficientemente uniforme. I titolari del trattamento dovrebbero avere una comprensione coerente di ciò che è «ragionevole e proporzionato», indipendentemente dal fatto che siano informati dalla giurisprudenza o dalle direttive di un'autorità di controllo, in quanto l'applicazione di questo concetto potrebbe potenzialmente portare a norme diverse nel rispetto del diritto di accesso, in particolare a seconda del livello di misure tecniche e organizzative che il titolare del trattamento ha messo in atto per gestire le richieste di accesso. L'EDPB apprezzerrebbe se la Commissione potesse fornire informazioni più dettagliate sull'interpretazione di «ricerche ragionevoli e proporzionate» sulla base degli orientamenti e della giurisprudenza nazionali disponibili. A fronte di un siffatto contesto, l'EDPB invita la Commissione a monitorare che il diritto di accesso non sia indebitamente limitato.

2.2.2. GARANZIE PER L'«ESENZIONE PER MOTIVI DI IMMIGRAZIONE»

35. La precedente cosiddetta «esenzione per motivi di immigrazione»⁽³¹⁾ consentiva ai titolari del trattamento coinvolti nel «controllo dell'immigrazione» di limitare alcuni diritti degli interessati previsti dalla DPA 2018, qualora ciò potesse pregiudicare talune attività di controllo dell'immigrazione⁽³²⁾. A causa di problemi di legittimità al momento dell'adozione della precedente decisione di adeguatezza del Regno Unito, il trattamento dei dati personali nell'ambito dell'esenzione è stato escluso dall'ambito di applicazione di tale decisione.
36. Dalla precedente decisione di adeguatezza del Regno Unito, l'esenzione per motivi di immigrazione è stata integrata due volte da garanzie⁽³³⁾. Esso comprende ora le seguenti garanzie: i) deve essere invocata solo caso per caso, ii) i diritti e le libertà dell'interessato e le potenziali vulnerabilità sono presi in considerazione iii) il segretario di Stato tiene un registro dell'applicazione dell'esenzione per motivi di immigrazione e informa generalmente l'interessato sul suo utilizzo e iv) chiarisce che l'applicazione dell'esenzione per motivi di immigrazione è limitata al trattamento da parte del segretario di Stato (compresi il ministero dell'Interno del Regno Unito e le sue agenzie). Inoltre, è stato specificato il necessario esercizio di bilanciamento per determinare se l'esercizio dei diritti dell'interessato possa pregiudicare l'effettivo controllo dell'immigrazione. L'ICO ha inoltre pubblicato orientamenti dettagliati sul ricorso all'esenzione. Nei suoi orientamenti, ha confermato l'interpretazione restrittiva dell'esenzione e che le restrizioni derivanti dall'esenzione per motivi di immigrazione dovrebbero essere applicate solo selettivamente a specifici diritti degli interessati. Ha inoltre affermato che, nell'effettuare il test comparativo, i titolari del trattamento devono garantire che il rischio per il controllo dell'immigrazione sia sostanziale e superiore al rischio per gli interessi della persona.
37. L'EDPB prende atto dell'analisi dettagliata della Commissione. Nel contesto delle controversie giuridiche che hanno preceduto tali modifiche, l'EDPB incoraggia la Commissione a monitorarne l'ulteriore applicazione.

intraprendere l'azione richiesta; oppure b) rifiutare di soddisfare la richiesta. Incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

⁽³¹⁾ Cfr. l'allegato 2 della DPA 2018, parte 1, della versione precedente della DPA.

⁽³²⁾ Cfr. i punti 61 e 62 del parere 14/2021 dell'EDPB: «pregiudicherebbero il mantenimento di un efficace controllo sull'immigrazione» o «l'indagine o la rilevazione di attività che potrebbero compromettere il mantenimento dell'effettivo controllo dell'immigrazione».

⁽³³⁾ Mediante regolamenti nel 2022 e nel 2024.

2.3. LIMITAZIONI AI TRASFERIMENTI SUCCESSIVI

38. L'EDPB accoglie con favore la costante attenzione della Commissione all'applicazione pratica delle norme del Regno Unito sui trasferimenti di dati personali verso paesi terzi e invita la Commissione a mantenere e intensificare tale impegno. Ciò è particolarmente importante per quanto riguarda l'autorità del segretario di Stato di emanare nuovi regolamenti mirati per approvare i trasferimenti i) a un settore o a un'area geografica di un paese terzo; ii) a uno specifico titolare del trattamento o responsabile del trattamento; iii) a un destinatario specifico dei dati personali; iv) di determinati tipi specifici di dati personali; v) effettuati con determinati mezzi specifici; o vi) sulla base di legislazione, sistemi, elenchi o altri accordi o documenti pertinenti, poiché hanno effetto di volta in volta; e per conferire un potere discrezionale a una persona (articolo 45 A, paragrafo 4, del RGPD del Regno Unito).
39. L'EDPB comprende che l'articolo 45 A, paragrafo 4, del RGPD del Regno Unito è inteso a consentire flessibilità per approvare determinati trasferimenti. Ad esempio, per quanto riguarda i punti ii) e iii), l'EDPB comprende che essi potrebbero riguardare i trasferimenti a soggetti privati in un paese terzo. Ciò significherebbe che tali soggetti privati si impegnano a rispettare la verifica della protezione dei dati. Non è chiaro in che modo il segretario di Stato possa valutare nella pratica che specifici titolari del trattamento stabiliti in un paese terzo – non considerati adeguati – possano conformarsi alla verifica della protezione dei dati (ad esempio per quanto riguarda il ricorso). Analogamente, non è chiaro come sarà effettuata la verifica della protezione dei dati per l'articolo 45 A, paragrafo 4, punti iv) e v), del RGPD del Regno Unito.
40. L'EDPB gradirebbe che la Commissione fornisse ulteriori dettagli sulle ulteriori informazioni e garanzie ricevute in merito all'applicazione pratica della verifica della protezione dei dati e spiegasse la sua valutazione in merito al modo in cui il livello di protezione è mantenuto in tali situazioni ⁽³⁴⁾. L'EDPB invita inoltre la Commissione a monitorare attentamente gli sviluppi nell'applicazione di questa disposizione.
41. Inoltre, l'EDPB comprende dalle informazioni supplementari fornite dalla Commissione che il criterio dell'opportunità di agevolare i trasferimenti di dati personali da e verso il Regno Unito non è un elemento della verifica della protezione dei dati, ma semplicemente un fattore aggiuntivo che il segretario di Stato può considerare qualora i criteri della verifica siano pienamente soddisfatti. L'EDPB invita la Commissione a chiarire questo punto nella sua decisione di adeguatezza finale, in quanto non è del tutto chiaro dal testo della legge, nonché a monitorare le relative implicazioni pratiche e l'attuazione di tale criterio.
42. Per quanto riguarda la nuova verifica della protezione dei dati introdotto dalla DUAA ⁽³⁵⁾, l'EDPB osserva che il nuovo elenco indicativo di elementi da prendere in considerazione nella verifica di adeguatezza non è esaustivo e che la nuova verifica di adeguatezza prevede che il livello di protezione degli interessati nei paesi terzi destinatari o nelle organizzazioni internazionali «non sia sostanzialmente inferiore» a quello previsto per gli interessati dalla pertinente legislazione del Regno Unito in materia di protezione dei dati. L'elenco elimina elementi importanti che figuravano nella precedente verifica di adeguatezza del Regno Unito e che svolgono un ruolo importante nel valutare se un paese terzo offra un livello sostanzialmente equivalente di protezione dei dati personali. La nuova verifica non fa più riferimento i) alle norme del paese terzo in materia di «sicurezza pubblica, difesa, sicurezza nazionale e diritto penale e accesso ai dati personali da parte delle autorità pubbliche», ii) alla giurisprudenza (ora la nuova verifica fa riferimento alla «costituzione, alle tradizioni e alla cultura

⁽³⁴⁾ Cfr. l'articolo 45 A), paragrafo 4, del RGPD del Regno Unito.

⁽³⁵⁾ Cfr. il considerando 42 del progetto di decisione.

del paese»), iii) all'esistenza di diritti effettivi e azionabili di cui godono gli interessati e ai mezzi di ricorso amministrativi e giudiziari che gli interessati i cui dati personali sono trasferiti possono effettivamente proporre (la nuova verifica fa invece riferimento b) all'esistenza, e ai poteri di un'autorità responsabile dell'applicazione della protezione degli interessati in relazione al trattamento dei dati personali nel paese o da parte dell'organizzazione, c) alle modalità di ricorso giurisdizionale o non giurisdizionale degli interessati in relazione a tale trattamento) e iv) a una o più autorità di controllo indipendenti (mentre la nuova verifica si riferisce a «un'autorità responsabile dell'applicazione della protezione degli interessati in relazione al trattamento dei dati personali nel paese o da parte dell'organizzazione»).

43. Pur riconoscendo che i criteri di riferimento per l'adeguatezza ai sensi del RGPD forniscono soltanto dettagli limitati su questo aspetto, l'EDPB ricorda il suo riferimento al fatto che il «livello di protezione delle persone fisiche i cui dati sono trasferiti non deve essere compromesso dal trasferimento successivo» ⁽³⁶⁾, che non può essere interpretato come se non includesse la necessità di un'autorità di controllo indipendente e diritti efficaci e applicabili degli interessati.
44. L'EDPB incoraggia la Commissione a sviluppare ulteriormente in modo specifico la sua valutazione su tali aspetti. Tale chiarimento garantirebbe una grande certezza giuridica e contribuirebbe a rafforzare la fiducia nello strumento di adeguatezza. L'EDPB invita inoltre la Commissione a monitorare attentamente gli sviluppi e l'attuazione pratica della nuova verifica di adeguatezza.
45. Per quanto riguarda l'adesione (associata) del Regno Unito al CBPR, l'EDPB osserva che l'attuale adesione non comporta alcuna agevolazione dei trasferimenti di dati dal Regno Unito ad altri membri del forum CBPR. L'EDPB accoglie con favore la posizione adottata dalla Commissione a tale riguardo, compreso l'impegno a continuare a monitorare attentamente gli ulteriori sviluppi al riguardo, in particolare se il Regno Unito intende progredire verso un'adesione a pieno titolo, e ricorda che le CBPR non sono riconosciute come garanzie di un livello sufficiente di protezione dei dati personali provenienti dall'UE.

2.4. PROCESSO DECISIONALE AUTOMATIZZATO

46. L'EDPB prende atto dell'articolo 80 della DUAA (che introduce articoli dal 22 A al 22 D del RGPD del Regno Unito), che apporta modifiche significative al quadro che disciplina il processo decisionale automatizzato, in particolare quando si basa sul trattamento di categorie non particolari di dati. Fino all'adozione della DUAA, l'articolo 22 del RGPD del Regno Unito corrispondeva al quadro dell'UE in materia di protezione dei dati con un divieto generale di processo decisionale automatizzato con limitate eccezioni.
47. L'articolo 22 B, paragrafo 1, del RGPD del Regno Unito vieta il trattamento di categorie particolari di dati personali per quelle decisioni basate esclusivamente su un trattamento automatizzato che hanno effetti giuridici o altrettanto significativi per l'interessato, con determinate eccezioni (articolo 22 B, paragrafi 2 e 3, del RGPD del Regno Unito, anche quando il trattamento è basato sul consenso, sul contratto o richiesto dalla legge).
48. L'EDPB osserva che tale divieto non si applica quando i titolari del trattamento prendono decisioni significative utilizzando processi automatizzati basati su categorie non particolari di dati, a meno che

⁽³⁶⁾ Cfr. il capitolo 3: principi generali di protezione dei dati per garantire che il livello di protezione in un paese terzo, in un territorio o in uno o più settori specifici all'interno di tale paese terzo o organizzazione internazionale sia sostanzialmente equivalente a quello garantito dalla legislazione dell'UE riguardante i criteri di riferimento per l'adeguatezza ai sensi del RGPD.

la base giuridica del trattamento non sia un interesse legittimo riconosciuto a norma dell'articolo 6, paragrafo 1, lettera e A), del RGPD del Regno Unito.

49. L'enfasi della legge passa dalla limitazione del ricorso al processo decisionale automatizzato alla certezza dell'esistenza di garanzie per decisioni importanti. Tali garanzie comprendono i) la fornitura all'interessato di informazioni sul processo decisionale, ii) la possibilità di presentare osservazioni in merito alla decisione ⁽³⁷⁾, iii) la contestazione di tale decisione e iv) la possibilità per l'interessato di richiedere l'intervento umano da parte del titolare del trattamento. L'EDPB osserva che, sebbene questo nuovo approccio rappresenti una deroga al precedente quadro giuridico, l'articolo 22 C del RGPD del Regno Unito impone ai titolari del trattamento di porre in essere garanzie adeguate che assicurino un livello adeguato di protezione per gli interessati.
50. Alla luce del contesto normativo in rapida evoluzione e dei progressi nelle tecnologie automatizzate, come l'IA, l'EDPB esorta la Commissione ad ampliare, nella sua decisione di adeguatezza finale, la valutazione degli impatti pratici previsti di questo nuovo approccio, che non è ancora stato messo alla prova nella pratica, nonché a monitorarne l'attuazione.

2.4.1. PROCESSO DECISIONALE AUTOMATIZZATO E COINVOLGIMENTO UMANO

51. L'EDPB accoglie con favore il chiarimento relativo al significato del processo decisionale automatizzato e del coinvolgimento umano. L'articolo 22 A del RGPD del Regno Unito chiarisce che una decisione basata esclusivamente su un trattamento automatizzato significa che non vi è un coinvolgimento umano significativo nel processo decisionale. Inoltre, i titolari del trattamento sono tenuti a valutare l'incidenza della profilazione in una decisione onde stabilire se l'intervento umano sia stato significativo.
52. Inoltre, l'articolo 22 D del RGPD del Regno Unito conferisce al segretario di Stato il potere di specificare mediante regolamenti se vi sia o meno un coinvolgimento umano significativo nell'adozione della decisione descritta nel regolamento. Parimenti, il segretario di Stato ha anche il potere di descrivere se si ritiene o meno che la decisione di cui al regolamento abbia un effetto analogamente significativo sugli interessati.
53. L'ambito e la discrezionalità di tali poteri non sono chiari. L'EDPB invita pertanto la Commissione ad analizzare questi nuovi poteri conferiti al segretario di Stato e a monitorare eventuali sviluppi al riguardo. D'altro canto, i poteri aggiuntivi del segretario di Stato per quanto riguarda le garanzie richieste dall'articolo 22 C del RGPD del Regno Unito, costituiscono un cambiamento positivo in quanto integrano e/o completano le garanzie già richieste e determinano quali garanzie sono insufficienti.

⁽³⁷⁾ Ossia fornire ulteriori informazioni e motivazioni, che non costituiscono ancora un ricorso giuridico formale.

3. MECCANISMO DI PROCEDURA E APPLICAZIONE

3.1. VIGILANZA E APPLICAZIONE

3.1.1. VIGILANZA INDIPENDENTE

54. L'EDPB osserva che, con l'entrata in vigore della DUAA ⁽³⁸⁾, l'ICO, precedentemente strutturato come un'entità distinta, verrà ristrutturato mediante l'introduzione di un organismo (un comitato), vale a dire l'Information Commissioner ai sensi dell'articolo 148 e dell'allegato 12A della DPA 2018.
55. L'EDPB rileva che la ristrutturazione di un'autorità da entità distinta a comitato non pregiudica di per sé l'indipendenza dell'autorità e la sua efficace applicazione. Si dovrebbe prestare attenzione ad altri elementi, quali le norme relative alla nomina e alla revoca, e, a tal proposito, l'EDPB accoglie con favore il fatto che solo Sua Maestà possa rimuovere il presidente dell'Information Commissioner dalla sua carica a seguito della raccomandazione di entrambe le camere del parlamento del Regno Unito in caso di colpa grave.
56. Norme dettagliate sul lavoro e sul funzionamento del nuovo Information Commissioner sono contenute nell'allegato 12A della DPA 2018. Esso disciplina, tra l'altro, il quadro strutturale e organizzativo dell'Information Commissioner, i requisiti per la nomina dei suoi membri esecutivi e non esecutivi nonché di altro personale (dipendenti e comitato esterno) e comprende disposizioni in materia di mandato, retribuzione, gestione dei conti e revoca. I numeri 5 e 6 dell'allegato 12A ⁽³⁹⁾ contengono norme e garanzie che devono essere rispettate nella nomina di membri non esecutivi e che potrebbero essere pertinenti per la costituzione dell'organismo e la sua indipendenza (ad es. selezione in base al merito e al conflitto di interessi).
57. L'EDPB osserva che il progetto di decisione non fornisce dettagli riguardo alle modifiche che pertengono al funzionamento della nuova autorità per la protezione dei dati. Inoltre, non vi sono dettagli sulla procedura per la nomina e la revoca dei membri esecutivi e non esecutivi. Poiché questi elementi sono pertinenti per la valutazione del meccanismo di vigilanza, l'EDPB invita la Commissione a descrivere ulteriormente le modifiche e la relativa valutazione, in particolare per quanto riguarda la struttura e l'organizzazione dell'Information Commissioner, la nomina e la revoca dei suoi membri, compreso quello non esecutivo.
58. Per quanto riguarda l'indipendenza dell'Information Commissioner, l'EDPB osserva che, ai sensi dell'allegato 12A, articolo 6, della DPA 2018, i conflitti di interesse possono impedire la nomina da parte del segretario di Stato in qualità di presidente o di membro non esecutivo dell'Information Commissioner. Nello specificare l'espressione «conflitto di interessi», l'articolo 6, paragrafo 5, fa riferimento a un interesse finanziario o di altro tipo che possa influire in modo preventivo sull'adempimento da parte della persona della sua funzione di membro della commissione. Per quanto riguarda l'indipendenza dei membri dell'Information Commissioner, tale «altro interesse», ad esempio una particolare prossimità economica e/o rapporti commerciali, può indicare anche conflitti di interessi e dovrebbe essere preso in considerazione nella procedura di nomina dei membri dell'Information Commissioner. L'EDPB invita pertanto la Commissione a monitorare che le restrizioni si applichino nella pratica.

⁽³⁸⁾ Cfr. la parte 6 «La Commissione d'informazione», DUAA n. 117, pagg. 133 e seguenti.

⁽³⁹⁾ Cfr. l'allegato 12A della DPA 2018.

59. In relazione agli obiettivi aggiornati di cui l'Information Commissioner deve tenere conto nello svolgimento dei propri compiti e nella preparazione della propria strategia, quali, tra l'altro, la promozione dell'innovazione e della concorrenza (articolo 120 B della DPA 2018), la Commissione ricorda che analogamente, la normativa dell'UE in materia di protezione dei dati bilancia anche la protezione dei dati personali con diversi altri diritti e obiettivi fondamentali e cita i considerando 2 e 4, nonché l'articolo 23 del RGPD. L'EDPB riconosce che la protezione dei dati non è un diritto assoluto e deve essere bilanciata con altri diritti e obiettivi fondamentali, conformemente al principio di proporzionalità. Tuttavia, l'EDPB osserva che i considerando 2 e 4 del RGPD, nonché l'articolo 23 del RGPD, differiscono da una disposizione giuridica che richiede espressamente alle autorità preposte alla protezione dei dati di tenere conto di una serie di obiettivi nell'esercizio delle loro funzioni. Per motivi di chiarezza, l'EDPB invita la Commissione a riformulare questo considerando per evitare di dare l'impressione che i considerando 2 e 4, nonché l'articolo 23, del RGPD abbiano lo stesso significato dell'articolo 120 B della DPA 2018 e a monitorare che l'attuazione di questi obiettivi aggiornati non porti nella pratica a un eccessivo squilibrio a scapito del diritto ai dati personali che pregiudicherebbe il livello di protezione dei dati personali.

3.1.2. APPLICAZIONE, COMPRESSE LE SANZIONI

60. L'EDPB accoglie con favore il fatto che la disposizione contenuta nel precedente progetto di legge di riforma del quadro sulla protezione dei dati del Regno Unito [il progetto di legge sulla protezione dei dati e sulle informazioni digitali (Data Protection and Digital Information Bill, «progetto di legge DPDI»⁽⁴⁰⁾)] e che stabilisce che l'ICO deve prendere in considerazione il parere del segretario di Stato nell'esercizio dei suoi poteri non sia più inclusa nel nuovo quadro in materia di protezione dei dati.
61. L'EDPB ritiene inoltre positivo che, dall'adozione della precedente decisione di adeguatezza del Regno Unito, l'ICO abbia pubblicato numerosi e utili codici di prassi, linee guida, pareri e altri documenti di orientamento per le parti interessate.
62. Come nel suo parere 14/2021⁽⁴¹⁾, l'EDPB sottolinea che un meccanismo di controllo efficace che consenta un'indagine indipendente sui reclami, nonché procedure di ricorso amministrativo e giudiziario efficaci sono elementi fondamentali per valutare se un sistema di protezione dei dati offra un livello di protezione adeguato. Inoltre, il fatto che esistano sanzioni efficaci è importante per garantire il rispetto delle norme.
63. In tale contesto, l'EDPB richiama l'attenzione della Commissione sulla consultazione pubblica pubblicata dall'ICO il 22 agosto in merito alle sue proposte di gestione dei reclami⁽⁴²⁾, che è stata avviata solo dopo la pubblicazione del progetto di decisione della Commissione. Nella sua introduzione⁽⁴³⁾ alle proposte della consultazione pubblica, l'ICO afferma di attendersi che, una volta entrata in vigore la DUAA, un maggior numero di reclami sarà risolto dalle organizzazioni stesse senza il coinvolgimento dell'ICO. Il contesto alla base di tale valutazione dell'ICO è che la DUAA stabilisce nuovi requisiti affinché le organizzazioni introducano una procedura di reclamo specificamente per le questioni relative alla protezione dei dati. L'articolo 164 A della DPA 2018⁽⁴⁴⁾ stabilisce che i titolari

⁽⁴⁰⁾ Cfr. l'articolo 32, nuovo articolo 120 E, F, G e H del progetto di legge DPDI.

⁽⁴¹⁾ Cfr. il parere 14/2021 dell'EDPB, punti da 112 a 114.

⁽⁴²⁾ Cfr. la consultazione dell'ICO sui progetti di modifica delle modalità di gestione dei reclami in materia di protezione dei dati: <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/2025/08/ico-consultation-on-draft-changes-to-how-we-handle-data-protection-complaints/>; <https://ico.org.uk/media2/nrljbhr2/proposed-dpt-framework-20250822.pdf>.

⁽⁴³⁾ Cfr. la nota 41.

⁽⁴⁴⁾ Cfr. l'articolo 164 A della DPA 2018.

del trattamento devono adottare misure per aiutare le persone che desiderano presentare reclami relativi all'utilizzo dei loro dati personali. Ad esempio, devono fornire un modulo di reclamo che possa essere compilato elettronicamente e con altri mezzi, devono accusare ricezione dei reclami entro 30 giorni e «senza indebito ritardo» adottare misure adeguate per rispondere e informare il reclamante dell'esito del reclamo. Se i reclami devono essere trattati dall'ICO, le proposte avanzate per la consultazione pubblica dovrebbero costituire la base per la gestione dei reclami da parte dell'ICO. A questo proposito, l'ICO propone una sorta di sistema di triage, in base al quale i reclami devono essere trattati con priorità e risultati diversi. Ciò dovrebbe consentire all'ICO, in quanto autorità di regolamentazione strategica, di concentrare le proprie risorse sui rischi più importanti e di individuare i problemi sistemici in una fase precoce. La proposta dell'ICO stabilisce criteri in un elenco non esaustivo che possono aumentare o ridurre la probabilità che una denuncia sia portata avanti ulteriormente ⁽⁴⁵⁾.

64. Le modifiche descritte al paragrafo 57 possono comportare un diverso approccio dell'Information Commissioner alla gestione dei reclami. A causa dell'avvio della consultazione pubblica dopo l'emanazione del progetto di decisione della Commissione, tali modifiche non sono ancora state recepite nel progetto di decisione.
65. L'EDPB invita la Commissione a includere tale elemento nella sua valutazione e a dare seguito, in particolare, ai risultati della consultazione pubblica dell'ICO. Inoltre, l'EDPB invita la Commissione a monitorare attentamente la futura gestione dei reclami da parte dell'Information Commissioner per garantire che sia assicurato un livello equivalente di protezione.
66. L'EDPB osserva inoltre che gli ampi poteri normativi conferiti al segretario di Stato dalla DUAA, compreso il potere di adottare disposizioni giuridiche, possono avere implicazioni per il funzionamento del lavoro dell'Information Commissioner e dei suoi membri. L'EDPB fa riferimento, ad esempio, alla necessità che l'Information Commissioner consulti il segretario di Stato in relazione ad alcuni dei suoi compiti. In particolare, l'articolo 124 A della DPA 2018 ⁽⁴⁶⁾ prevede che l'Information Commissioner stabilisca codici di buone pratiche adeguati contenenti linee guida per il corretto trattamento dei dati personali, ove richiesto da un regolamento adottato dal segretario di Stato. L'Information Commissioner è tenuta a consultare il segretario di Stato prima di modificare o sviluppare tali codici.
67. Data l'importanza dell'indipendenza dell'Information Commissioner, l'EDPB invita la Commissione a monitorare attentamente questi nuovi poteri del segretario di Stato, in particolare il loro effetto pratico sul lavoro dell'Information Commissioner.
68. Come già sottolineato dall'EDPB nel parere 14/2021, l'ICO è adeguatamente dotato dei poteri necessari, che corrispondono in gran parte ai poteri delle autorità di controllo degli Stati membri dell'UE di cui all'articolo 58 del RGPD. Allo stesso tempo, come già evidenziato dall'EDPB, l'esistenza di sanzioni efficaci svolge un ruolo importante nel garantire il rispetto delle norme. L'EDPB invita la Commissione a effettuare una valutazione approfondita e a monitorare l'applicazione dei poteri correttivi, l'efficacia delle sanzioni e dei mezzi di ricorso per le parti interessate nell'ambito del quadro sulla protezione dei dati del Regno Unito ⁽⁴⁷⁾.

⁽⁴⁵⁾ [Cfr. la nota 41.](#)

⁽⁴⁶⁾ Codice di pratiche per il trattamento dei dati personali.

⁽⁴⁷⁾ Cfr. il parere 14/2021 dell'EDPB, punto 113.

4. DATI PERSONALI: ACCESSO E UTILIZZO SE TRASFERITI DA AUTORITÀ PUBBLICHE DALL'UNIONE EUROPEA AL REGNO UNITO

69. Il progetto di decisione si concentra sugli sviluppi pertinenti per la valutazione del livello di protezione nel Regno Unito dall'adozione della precedente decisione di adeguatezza del Regno Unito, che rimane valida per gli aspetti del quadro sulla protezione dei dati del Regno Unito che non sono stati modificati o interessati. Questo approccio generale riguarda anche l'analisi della Commissione relativa all'accesso ai dati personali e al loro utilizzo da parte delle autorità pubbliche nel Regno Unito. Questo aspetto specifico è spesso denominato «accesso da parte di pubbliche amministrazioni» ed è uno degli elementi elencati nell'articolo 45, paragrafo 2, lettera a), del RGPD, di cui la Commissione deve tenere conto nel determinare se il livello di protezione è essenzialmente equivalente.
70. In tale contesto, le sezioni seguenti affrontano una serie di punti specifici sollevati nel progetto di decisione attualmente in esame che sono pertinenti per quanto riguarda i dati personali trasferiti dal SEE ai sensi della decisione di adeguatezza del RGPD del Regno Unito e consultati e trattati dalle autorità pubbliche nel Regno Unito, compresi i trasferimenti successivi. L'analisi e le osservazioni dell'EDPB di cui al parere 14/2021 ⁽⁴⁸⁾ rimangono generalmente valide.

4.1. ACCESSO E USO DA PARTE DELLE AUTORITÀ PUBBLICHE DEL REGNO UNITO A FINI DI CONTRASTO PENALE

71. Il quadro di protezione dei dati che disciplina l'accesso e l'uso da parte delle autorità pubbliche del Regno Unito a fini di contrasto penale è stato oggetto di modifiche legislative rispetto alla precedente valutazione della Commissione contenuta nella precedente decisione di adeguatezza del Regno Unito, tra cui la legge del 2023 sulla sicurezza nazionale, l'IPAA 2024 e l'introduzione della DUAA. Quest'ultimo aspetto è affrontato anche nel progetto di decisione della Commissione che modifica la decisione di esecuzione (UE) 2021/1773, nonché nel corrispondente parere dell'EDPB emesso sulla base dell'articolo 51, paragrafo 1, lettera g), della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie.

4.1.1. BASI GIURIDICHE E GARANZIE APPLICABILI

4.1.1.1. POTERI DI INDAGINE A FINI DI CONTRASTO

72. Nei considerando da 81 a 85 del progetto di decisione, la Commissione delinea le modifiche all'IPA 2016 introdotte dall'IPAA 2024, nella misura in cui riguardano il trattamento a fini di contrasto ⁽⁴⁹⁾. Nel complesso, la Commissione fornisce informazioni dettagliate. Tuttavia, per quanto riguarda una modifica specifica, l'EDPB ritiene che al progetto di decisione giovinno ulteriori chiarimenti.
73. L'IPAA 2024 ha rivisto la definizione di «operatore di telecomunicazioni», ossia i potenziali destinatari di un avviso di conservazione ai sensi dell'IPA 2016 ⁽⁵⁰⁾. La definizione modificata comprende ora

⁽⁴⁸⁾ Cfr. il parere 14/2021 dell'EDPB.

⁽⁴⁹⁾ La Commissione evidenzia che, come descritto nei considerando da 139 a 141 della decisione di esecuzione (UE) 2021/1772, specifiche autorità di contrasto possono anche utilizzare poteri di indagine mirati nell'ambito dell'IPA 2016 ai fini della prevenzione o dell'individuazione di reati gravi. Le modifiche a tali disposizioni riguardano pertanto non solo l'accesso ai dati a fini di sicurezza nazionale, ma anche a fini di contrasto.

⁽⁵⁰⁾ Articolo 261, paragrafo 10, lettera c), dell'IPA 2016, inserito dall'articolo 19 dell'IPAA 2024.

qualsiasi persona che controlla o fornisce un sistema di telecomunicazioni che i) non è (in tutto o in parte) nel Regno Unito o da esso controllato e ii) è utilizzato da un'altra persona per offrire o fornire un servizio di telecomunicazione a persone nel Regno Unito. Sebbene la Commissione faccia riferimento alle note esplicative dell'IPAA 2024, in cui si afferma che l'articolo 261, paragrafo 10, lettera c), fornisce ulteriori chiarimenti per garantire che le grandi imprese con strutture societarie complesse siano coperte nella loro totalità dall'IPA 2016, e che la modifica non intende far rientrare altre imprese nell'ambito di applicazione, le implicazioni di tale cambiamento rimangono poco chiare, ad esempio se è suscettibile di ampliare il volume di dati personali potenzialmente soggetto a un avviso di conservazione. L'EDPB invita pertanto la Commissione ad affrontare più dettagliatamente gli effetti di tale modifica e a monitorare specificamente tale aspetto, in particolare alla luce dei principi di necessità e proporzionalità.

4.1.1.2. ESENZIONI PER MOTIVI DI SICUREZZA NAZIONALE PER LE AUTORITÀ DI CONTRASTO

74. L'articolo 88 della DUAA aggiorna le esenzioni per motivi di sicurezza nazionale esistenti nell'ambito del quadro di contrasto per rispecchiare quelle disponibili nell'ambito del RGPD del Regno Unito e dei regimi dei servizi di intelligence ⁽⁵¹⁾. Sebbene le autorità di contrasto siano già in grado di limitare determinati obblighi per motivi di protezione della sicurezza nazionale, come quelli relativi ai diritti degli interessati, l'articolo 78 A della DPA 2018 includerà ⁽⁵²⁾ anche la maggior parte dei principi di protezione dei dati ⁽⁵³⁾ e alcuni requisiti in materia di trasferimento internazionale dei dati ⁽⁵⁴⁾ come disposizioni che possono essere disapplicate se necessario ai fini della salvaguardia della sicurezza nazionale. Inoltre, alcuni dei poteri di accesso dell'Information Commissioner per effettuare ispezioni e adottare misure di esecuzione ⁽⁵⁵⁾ possono essere disapplicati in tali circostanze.
75. Tali modifiche non sono menzionate né nel progetto di decisione di adeguatezza ai sensi dell'articolo 45 del RGPD né nel progetto di decisione di adeguatezza ai sensi dell'articolo 36 della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie. Tuttavia, l'EDPB considera essenziale valutare tali esenzioni estese alla luce dei principi di necessità e proporzionalità. In tale contesto, l'EDPB ricorda la seconda delle quattro cosiddette «garanzie essenziali europee»: qualsiasi limitazione all'esercizio dei diritti e delle libertà riconosciuti dalla Carta deve rispettarne il contenuto essenziale e, nel rispetto del principio di proporzionalità, può essere apportata solo se necessaria e realmente rispondente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui ⁽⁵⁶⁾. L'EDPB nutre preoccupazioni riguardo alle esenzioni ai principi fondamentali in materia di protezione dei dati, ai requisiti di trasferimento internazionale e ai poteri dell'Information Commissioner.

⁽⁵¹⁾ Cfr. anche la scheda informativa del dipartimento per la Scienza, l'innovazione e la tecnologia, i dati (uso e accesso): RGPD del Regno Unito e DPA, pubblicata il 27 giugno 2025, pag. 14 <https://www.gov.uk/government/publications/data-use-and-access-act-2025-factsheets/data-use-and-access-act-factsheet-uk-gdpr-and-dpa>.

⁽⁵²⁾ Il DUAA sarà introdotto gradualmente in più fasi. Le principali modifiche alla legislazione in materia di protezione dei dati nella parte 5 della DUAA entreranno in vigore nell'ambito della fase 3, circa sei mesi dopo l'assenso reale (<https://www.gov.uk/guidance/data-use-and-access-act-2025-plans-for-commencement>).

⁽⁵³⁾ Cfr. articolo 78 A, paragrafo 1, paragrafo 2, lettera a) e paragrafo 3, della DPA 2018, introdotto dall'articolo 88 della DUAA.

⁽⁵⁴⁾ Cfr. l'articolo 78 A, paragrafo 1, paragrafo 2, lettera a), e paragrafo 4, della DPA 2018, introdotto dall'articolo 88 della DUAA.

⁽⁵⁵⁾ Cfr. l'articolo 78 A, paragrafo 1, paragrafo 2, lettere e), f) e g), della DPA 2018, introdotto dall'articolo 88 della DUAA.

⁽⁵⁶⁾ Cfr. le raccomandazioni 2/2020 dell'EDPB relative alle garanzie essenziali europee per le misure di sorveglianza, adottate il 10 novembre 2020, pag. 10.

76. In base alla norma rivista, cinque dei sei principi di protezione dei dati possono essere disapplicati, ove necessario, per salvaguardare la sicurezza nazionale ⁽⁵⁷⁾. Tali principi stabiliscono, tra l'altro, che la finalità di contrasto per la quale i dati personali sono raccolti deve essere determinata, esplicita e legittima e che i dati personali devono essere adeguati, pertinenti e non eccedenti rispetto a tale finalità. Essi specificano inoltre che i dati personali devono essere esatti e conservati solo per il tempo necessario. Come indicato in precedenza, le future esenzioni comprendono anche alcuni dei requisiti relativi ai trasferimenti internazionali, come la cosiddetta seconda condizione per i trasferimenti internazionali di cui all'articolo 73, paragrafo 3, della DPA 2018. Questa condizione richiede che i trasferimenti siano basati su norme di adeguatezza, garanzie adeguate o, se nessuna di queste è applicabile, su circostanze particolari. Le esenzioni incidono anche sui poteri dell'Information Commissioner, ad esempio l'autorità di emettere informazioni e notifiche di esecuzione ⁽⁵⁸⁾.
77. L'EDPB osserva che, sebbene si discostino chiaramente dalla direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, le esenzioni sono molto simili alle eccezioni e alle restrizioni in materia di sicurezza nazionale previste dall'articolo 11 della convenzione 108 modernizzata del Consiglio d'Europa («convenzione 108+») ⁽⁵⁹⁾, firmata dal Regno Unito il 10 ottobre 2018 ma che, alla data del presente parere, non è stata ancora ratificata dal Regno Unito o non è ancora entrata in vigore ⁽⁶⁰⁾. A tale riguardo, l'EDPB ricorda che il comitato consultivo della convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale (T-PD) ha recentemente pubblicato orientamenti sui principi generali di cui all'articolo 11 della convenzione 108 modernizzata ⁽⁶¹⁾.
78. Nei suoi orientamenti, il Consiglio d'Europa sottolinea esplicitamente che nessuna eccezione è applicabile, tra l'altro, per la proporzionalità e la legittimità della finalità dei principi di trattamento. Ciò implica che deve essere garantita la proporzionalità del trattamento dei dati, nonché i requisiti per il trattamento dei dati personali per una finalità legittima. In linea con gli orientamenti del T-PD, l'EDPB rimane particolarmente vigile per quanto riguarda eventuali esenzioni rispetto al principio di proporzionalità, nonché al requisito di trattare i dati personali per una finalità legittima. Analogamente, a parere dell'EDPB, qualsiasi esenzione rispetto ai poteri dell'autorità di controllo dovrebbe essere affrontata con cautela. Se da un lato requisiti specifici per le attività di controllo, come i nulla osta di sicurezza, possono essere appropriati nel contesto del trattamento relativo alla sicurezza nazionale, dall'altro è essenziale garantire un controllo efficace per evitare la creazione di un vuoto di controllo. Nello stesso spirito, l'articolo 11, paragrafo 3, della convenzione 108+ stabilisce che le esenzioni al suo articolo 15 ⁽⁶²⁾ l'obbligo secondo cui le attività di trattamento per finalità di difesa e sicurezza nazionale siano soggette a un riesame e a una supervisione indipendenti ed efficaci ai sensi

⁽⁵⁷⁾ Ai sensi dell'articolo 78 A, paragrafi 2 e 3, della DPA 2018, il capo 2 della parte 3 di detta legge non si applica se necessario ai fini della salvaguardia della sicurezza nazionale, fatta eccezione per a) l'articolo 35, paragrafo 1 (il primo principio di protezione dei dati) nella misura in cui impone la liceità del trattamento dei dati personali; b) l'articolo 35, paragrafi da 2 a 5 (liceità del trattamento e restrizioni al trattamento sensibile); c) l'articolo 42 (garanzie: trattamento sensibile) e d) l'allegato 8 (condizioni per il trattamento sensibile).

⁽⁵⁸⁾ Gli avvisi di informazione impongono al titolare del trattamento o al responsabile del trattamento di fornire all'Information Commissioner le informazioni ragionevolmente necessarie per lo svolgimento delle sue funzioni. Gli avvisi di esecuzione consentono all'Information Commissioner di richiedere a una persona di adottare (o di astenersi dall'adottare) azioni specifiche, qualora l'Information Commissioner abbia accertato che la persona non rispetta particolari obblighi in materia di protezione dei dati.

⁽⁵⁹⁾ Cfr. il protocollo che modifica la convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale (STCE n. 223).

⁽⁶⁰⁾ <https://www.coe.int/en-GB/web/conventions/full-list?module=signatures-by-treaty&treatynum=223>

⁽⁶¹⁾ <https://rm.coe.int/t-pd-2021-7rev13-interpretation-of-general-principles-article-11-c108-/1680b6c146>

⁽⁶²⁾ Cfr. l'articolo 15 della convenzione 108+, che specifica in che modo le parti della convenzione, prevedendo una o più autorità di controllo, garantiscono il rispetto delle disposizioni della convenzione.

della legislazione nazionale delle parti della convenzione. Inoltre, qualsiasi esenzione dovrebbe essere interpretata nel modo più restrittivo possibile. Il fatto che i dati personali siano trattati a fini di sicurezza nazionale non dovrebbe essere di per sé sufficiente per invocare un'esenzione. Dovrebbe essere chiaro che un'esenzione dal regime di protezione dei dati deve essere applicata caso per caso e solo se ciò è necessario e proporzionato ⁽⁶³⁾.

79. Poiché i progetti di decisione di adeguatezza non affrontano questo punto, l'EDPB invita la Commissione a integrare la sua valutazione nel progetto di decisione e a monitorare specificamente l'applicazione pratica delle esenzioni per motivi di sicurezza nazionale per le autorità di contrasto.

4.1.2. CONTROLLI CONGIUNTI TRA LE AGENZIE DI INTELLIGENCE DEL REGNO UNITO E LE AUTORITÀ DI CONTRASTO

80. Sulla base delle modifiche apportate dalla DUAA, le attività di trattamento svolte dalle autorità competenti per le attività di contrasto, in circostanze specifiche possono rientrare nelle norme in genere applicabili al trattamento dei dati personali da parte delle autorità di sicurezza nazionale ⁽⁶⁴⁾. In altre parole, fatte salve le condizioni di cui all'articolo 89 della DUAA, il regime di protezione dei dati per i trattamenti a fini di sicurezza nazionale di cui alla parte 4 della DPA 2018 è esteso al trattamento dei dati da parte delle autorità di contrasto.
81. La Commissione sottolinea che le condizioni di cui all'articolo 89 della DUAA prevedono rigorose garanzie: un'autorità competente deve essere specificata come «autorità competente qualificata» nei regolamenti emanati dal segretario di Stato, che, inoltre, deve designare una particolare attività di trattamento svolta dall'autorità competente qualificata come contitolare del trattamento con almeno un servizio di intelligence ai fini della salvaguardia della sicurezza nazionale ⁽⁶⁵⁾.
82. Pur riconoscendo che tali garanzie comportano restrizioni significative, l'EDPB invita la Commissione a monitorare l'attuazione pratica di tali norme. Occorre prestare particolare attenzione a garantire che la parte 4 della DPA 2018 sia applicata rigorosamente alle operazioni di trattamento per finalità di sicurezza nazionale, senza essere estesa ad altri contesti. Sebbene agli Stati sia concesso un ampio margine di discrezionalità in materia di sicurezza nazionale, come riconosciuto anche dalla CEDU ⁽⁶⁶⁾, l'EDPB ritiene che le minacce alla sicurezza nazionale debbano essere distinguibili per la loro natura, la loro gravità e le circostanze specifiche dai rischi generali per la sicurezza pubblica o da reati gravi. Solo in tali casi l'attività delle autorità di contrasto nell'ambito del regime di protezione dei dati dei servizi di intelligence è compatibile con i principi di necessità e proporzionalità ⁽⁶⁷⁾. Inoltre, l'EDPB ritiene necessario monitorare se le autorità competenti qualificate siano in grado, nella pratica, di mantenere una chiara distinzione tra le diverse finalità di trattamento al fine di rispettare di conseguenza il corrispondente quadro giuridico.

⁽⁶³⁾ Cfr. anche l'articolo 11 della convenzione 108+, che specifica che le eccezioni devono essere previste dalla legge, rispettare l'essenza dei diritti e delle libertà fondamentali e costituire una misura necessaria e proporzionata in una società democratica. Secondo le linee guida del TP-D sui principi generali dell'articolo 11, ciò implica che deve essere effettuata e giustificata una ponderazione degli interessi in gioco tra la necessità di prevedere eccezioni a talune disposizioni della convenzione e il rispetto dei diritti umani e delle libertà fondamentali delle persone.

⁽⁶⁴⁾ Cfr. il considerando 72 del progetto di decisione.

⁽⁶⁵⁾ Cfr. il considerando 73 del progetto di decisione.

⁽⁶⁶⁾ Cfr. CEDU, *Big Brother Watch e a./Regno Unito*, 25 maggio 2021, punto 305.

⁽⁶⁷⁾ Dalla giurisprudenza della CGUE, nell'applicare la verifica di necessità e proporzionalità alla legislazione degli Stati membri che consente la conservazione dei dati personali e l'accesso agli stessi da parte delle autorità pubbliche, deriva che obiettivi legittimi, quali la sicurezza nazionale o la lotta contro reati gravi, sono diversi e potrebbero pertanto giustificare diversi tipi di ingerenza. Cfr. CGUE, cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e a.*, 6 ottobre 2020.

4.1.3. IL DIRITTO DI ACCESSO

83. La DUAA specifica che gli interessati hanno il diritto di accedere alle informazioni pertinenti solo nella misura in cui il titolare del trattamento sia in grado di fornirle sulla base di una ricerca ragionevole e proporzionata. Tale modifica è introdotta sia nel regime di contrasto che nel regime di sicurezza nazionale ⁽⁶⁸⁾.
84. La Commissione lo spiega come un chiarimento in linea con le norme consolidate elaborate nell'ambito della giurisprudenza nazionale, che tengono conto anche degli interessi dell'interessato. Tuttavia, l'EDPB avrebbe accolto con favore informazioni più dettagliate sull'interpretazione della nozione di «ricerca ragionevole e proporzionata», anche perché l'articolo 14 della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie non contiene tale elemento. L'EDPB riconosce che possono effettivamente esistere scenari in cui gli sforzi di un titolare del trattamento per individuare e localizzare le informazioni sull'interessato potrebbero essere considerati irragionevoli e sproporzionati senza compromettere l'equivalenza sostanziale ⁽⁶⁹⁾. L'EDPB ricorda l'analisi e la conclusione di cui al punto 34 del presente parere che sono ugualmente pertinenti per il regime di contrasto e di sicurezza nazionale.

4.1.4. TRASFERIMENTI SUCCESSIVI

4.1.4.1. UNA NUOVA VERIFICA DELLA PROTEZIONE DEI DATI

85. Quando un'autorità competente intende condividere dati personali trattati ai sensi della parte 3 della DPA 2018 con le autorità di contrasto di un paese terzo, si applicano requisiti specifici. In particolare, tali trasferimenti possono avvenire quando sono approvati da regolamenti emanati dal segretario di Stato o, in mancanza di tali regolamenti, sulla base di garanzie adeguate. Se un trasferimento non può basarsi su un regolamento né su garanzie adeguate, può avvenire solo in determinate circostanze specifiche, denominate «circostanze particolari» corrispondenti alle situazioni e alle condizioni che si qualificano come «deroghe» ai sensi dell'articolo 38 della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie.
86. Sebbene la Commissione osserva che il regime in materia di trasferimenti internazionali di dati personali dal Regno Unito è sostanzialmente identico alle norme stabilite al capo V della direttiva (UE) 2016/680, il progetto di decisione indica altresì che è stato riformulato il criterio giuridico in base al quale i regolamenti possono approvare i trasferimenti, a cui era fatto riferimento come regolamenti sull'adeguatezza nel precedente articolo 74 A della DPA 2018, e sono state riformulate garanzie adeguate. Aniché fare riferimento a un livello di protezione adeguato, la nuova «verifica della protezione dei dati» di cui all'articolo 74 AB della DPA 2018 richiede che il livello di protezione degli interessati nei paesi terzi destinatari o nelle organizzazioni internazionali «non sia sostanzialmente inferiore» a quello previsto per gli interessati dalla pertinente legislazione del Regno Unito in materia di protezione dei dati.
87. In tale contesto, l'EDPB rileva che gli elementi che il segretario di Stato deve prendere in considerazione nella valutazione di cui all'articolo 74 AB, paragrafo 2, della DPA 2018 sembrano essere

⁽⁶⁸⁾ Cfr. l'articolo 78, paragrafi 3 e 4, della DUAA, che modifica gli articoli 45 e 94 della DPA 2018.

⁽⁶⁹⁾ Ad esempio, si potrebbe sostenere che questo è il caso della ricerca di dispositivi sequestrati che non sono ancora stati analizzati o decrittati.

stati ridotti rispetto alla precedente valutazione dei regolamenti di adeguatezza ⁽⁷⁰⁾. L'EDPB sottolinea l'eliminazione di alcuni fattori che, a suo avviso, svolgono un ruolo importante nel valutare se un paese terzo offre un livello di protezione dei dati personali sostanzialmente equivalente e ricorda l'analisi e le conclusioni di cui ai punti 42-43 del presente parere. In particolare, l'EDPB i) incoraggia la Commissione ad affrontare in modo specifico le modifiche e a elaborare ulteriormente la sua valutazione della nuova verifica della protezione dei dati. L'EDPB è consapevole del fatto che le nuove norme sui trasferimenti di dati personali verso paesi terzi sono intese a fornire ulteriore flessibilità. Allo stesso tempo, l'EDPB invita la Commissione a monitorare l'applicazione pratica di tali norme nel settore del contrasto e della cooperazione giudiziaria penale. Ciò è particolarmente importante per quanto riguarda la nuova autorità del segretario di Stato di emanare regolamenti che individuino e approvino un trasferimento, sulla base della nuova verifica della protezione dei dati, con qualsiasi mezzo, anche con riferimento ai settori geografici all'interno di un paese, ai titolari o ai responsabili del trattamento, ai destinatari dei dati, ai tipi di dati, ai mezzi di trasferimento e agli strumenti giuridici. Non è ancora chiaro, ad esempio, in che modo uno specifico titolare del trattamento o responsabile del trattamento con sede in un paese terzo che non è considerato adeguato soddisferebbe la verifica della protezione dei dati quando si tratta di un ricorso effettivo o di diritti degli interessati non già stabiliti nel quadro giuridico di tale paese terzo.

88. Inoltre, l'EDPB ricorda le conclusioni di cui al punto 41 in relazione all'uso del criterio dell'«opportunità di facilitare i trasferimenti di dati personali da e verso il Regno Unito» (articolo 74 AA, paragrafo 3, della DPA 2018) e invita la Commissione a specificare nella sua decisione che tale criterio non è un elemento della verifica della protezione dei dati, ma semplicemente un fattore aggiuntivo che il segretario di Stato può prendere in considerazione laddove i criteri della verifica siano pienamente soddisfatti, in quanto ciò non risulta del tutto chiaro dal testo della legge. A tale riguardo, l'EDPB invita la Commissione a monitorare le implicazioni pratiche dell'articolo 74 AA, paragrafo 3, della DPA 2018, in quanto resta da vedere quale ruolo avrà l'«opportunità di facilitare i trasferimenti di dati personali da e verso il Regno Unito» in questo contesto.

4.1.4.2. ACCORDO TRA REGNO UNITO E STATI UNITI SULLA LEGGE CLOUD

89. Un altro importante sviluppo nel settore dei trasferimenti successivi è l'entrata in vigore, nell'ottobre 2022, dell'accordo tra il governo del Regno Unito di Gran Bretagna e Irlanda del Nord e il governo degli Stati Uniti d'America sull'accesso ai dati elettronici allo scopo di contrastare le forme gravi di criminalità («accordo tra Regno Unito e Stati Uniti sulla legge CLOUD»). Come giustamente rilevato dalla Commissione, i dati personali trasferiti dall'UE a prestatori di servizi nel Regno Unito potrebbero essere oggetto di ordini di produzione di prove emessi dalle autorità di contrasto statunitensi competenti ai sensi di tale accordo ⁽⁷¹⁾.
90. Dato che, al momento dell'adozione della precedente decisione di adeguatezza del Regno Unito, l'accordo era stato concluso ma non era ancora entrato in vigore, la Commissione ha sottolineato che qualsiasi informazione e futuro chiarimento sul modo in cui gli Stati Uniti rispetteranno i propri obblighi ai sensi dell'accordo dovrebbe essere comunicato dal Regno Unito alla Commissione al fine di garantire un adeguato monitoraggio della precedente decisione di adeguatezza del Regno Unito in linea con l'articolo 45, paragrafo 4, del RGPD. La Commissione ha osservato che occorre prestare particolare

⁽⁷⁰⁾ La disposizione di cui all'articolo 74 A, paragrafo 4, della DPA 2018, omessa dalla DUAA, prevedeva un elenco di criteri identici all'articolo 36, paragrafo 3, della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie.

⁽⁷¹⁾ Cfr. il considerando 87 del progetto di decisione.

attenzione all'applicazione e all'adeguamento delle garanzie stabilite nell'accordo quadro UE-USA ⁽⁷²⁾ al tipo specifico di trasferimenti contemplati dall'accordo tra Regno Unito e Stati Uniti sulla legge CLOUD ⁽⁷³⁾. Facendo seguito a tale dichiarazione, nel suo progetto di decisione la Commissione fa riferimento a diversi chiarimenti raggiunti tra il Regno Unito e gli Stati Uniti nel contesto dell'applicazione dell'accordo quadro UE-USA all'accordo tra Regno Unito e Stati Uniti sulla legge CLOUD. L'EDPB accoglie con favore tali chiarimenti, che forniscono ulteriore chiarezza giuridica. Allo stesso tempo, vale la pena osservare che l'accordo quadro UE-USA non è ancora stato riesaminato, il che limita in certa misura le conclusioni che possono essere tratte in merito all'impatto e all'efficacia della sua applicazione all'accordo tra Regno Unito e Stati Uniti sulla legge CLOUD ⁽⁷⁴⁾. Inoltre, visto l'accordo quadro UE-USA, l'EDPB desidera ricordare la necessità di migliorare il livello delle garanzie previste da tale accordo. Ciò vale in particolare per la disponibilità di mezzi di ricorso giurisdizionale. Gli interessati dell'UE diversi dai cittadini dell'UE non hanno alcuna base giuridica ai sensi della Judicial Redress Act, la legge sul ricorso giurisdizionale, per avvalersi dei mezzi di ricorso. Inoltre, la Privacy Act, la legge sulla privacy, contiene eccezioni, che non sono state modificate dalla legge sul ricorso giurisdizionale, che riducono la capacità delle persone di presentare ricorso in determinate situazioni di contrasto e di sicurezza nazionale. Sebbene la Commissione rilevi che la legge sul ricorso giurisdizionale non è l'unico meccanismo per presentare ricorso, il progetto di decisione si limita ad affermare che a seconda delle circostanze e del contesto del caso specifico, altre leggi applicabili degli Stati Uniti offrono vie alternative per l'eventuale ricorso giurisdizionale ⁽⁷⁵⁾. Resta da chiarire se tutte le persone fisiche dell'UE i cui dati possono essere soggetti all'accordo tra Regno Unito e Stati Uniti sulla legge CLOUD godranno di diritti di ricorso giurisdizionale negli Stati Uniti.

91. L'EDPB osserva inoltre che una specifica garanzia reciproca stabilita nell'accordo tra Regno Unito e Stati Uniti sulla legge CLOUD, in base al quale entrambe le parti limitano l'impatto che l'accordo può avere rispettivamente per i cittadini del Regno Unito e degli Stati Uniti, non è, per sua natura, applicabile ai cittadini dell'UE ⁽⁷⁶⁾. L'EDPB osserva che, per questo motivo, solide garanzie in materia di protezione dei dati sono essenziali per garantire che i diritti degli interessati dell'UE siano adeguatamente tutelati se trattati nell'ambito di tale accordo. Pertanto, l'EDPB invita la Commissione a continuare a includere l'accordo tra Regno Unito e Stati Uniti sulla legge CLOUD nelle valutazioni e nei suoi riesami futuri della decisione di adeguatezza.
92. Nel complesso, l'EDPB ritiene necessario chiarire la valutazione della Commissione dell'accordo tra Regno Unito e Stati Uniti sulla legge CLOUD e qualsiasi possibile impatto dell'accordo sul livello di protezione valutato nella precedente decisione di adeguatezza del Regno Unito. I risultati del primo riesame dell'accordo tra Regno Unito e Stati Uniti sulla legge CLOUD, che, ai sensi dell'articolo 12,

⁽⁷²⁾ Cfr. l'accordo tra gli Stati Uniti d'America e l'Unione europea sulla protezione delle informazioni personali a fini di prevenzione, indagine, accertamento e perseguimento di reati, GU L 336 del 10.12.2016, pagg. 3-13, [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01)).

⁽⁷³⁾ Cfr. il considerando 155 della decisione di esecuzione (UE) 2021/1772. Ai sensi dell'articolo 9, paragrafo 1, dell'accordo tra Regno Unito e Stati Uniti sulla legge CLOUD, l'accordo quadro UE-USA si applica mutatis mutandis all'accordo tra Regno Unito e Stati Uniti sulla legge CLOUD. Esso può essere applicato solo mutatis mutandis, in quanto l'accordo quadro disciplina i trasferimenti transfrontalieri tra le autorità di contrasto e non la cooperazione diretta tra un prestatore di servizi e un'autorità di contrasto.

⁽⁷⁴⁾ Cfr. l'articolo 23 dell'accordo quadro UE-USA, a norma del quale le parti effettuano riesami periodici congiunti delle politiche e delle procedure che attuano l'accordo, il primo dei quali avviene non oltre tre anni dalla data di entrata in vigore dell'accordo. L'accordo quadro UE-USA è entrato in vigore nel febbraio 2017.

⁽⁷⁵⁾ Cfr. il considerando 93 del progetto di decisione.

⁽⁷⁶⁾ Cfr. l'articolo 4, paragrafo 3, e l'articolo 7, paragrafo 1, dell'accordo, che prevedono restrizioni mirate e stabiliscono che le ordinanze oggetto dell'accordo non possono essere intenzionalmente rivolte a una «persona della parte ricevente». Pertanto, gli Stati Uniti non possono intenzionalmente riferirsi a una persona situata nel territorio del Regno Unito e il Regno Unito deve rispettare una restrizione analoga.

paragrafo 1, dell'accordo, devono essere effettuati entro un anno dall'entrata in vigore dell'accordo, potrebbero essere particolarmente utili per tali ulteriori analisi.

4.1.5. VIGILANZA E RICORSO

93. L'EDPB nota che il sistema di vigilanza degli enti di contrasto in materia penale ai sensi della DPA 2018 e dell'IPA 2016, nonché i meccanismi di ricorso disponibili ai sensi della parte 3 della DPA 2018, dell'IPA 2016 e della Human Rights Act, la legge del 1998 sui diritti umani, rimangono in gran parte invariati. In particolare, la vigilanza nel Regno Unito continua a essere assicurata, oltre che dall'ICO, da una combinazione di diversi Commissioner, vale a dire l'Investigatory Powers Commissioner, IPC), assistito da altri commissari giudiziari, nonché il Biometrics and Surveillance Camera Commissioner.
94. Come spiegato dalla Commissione al considerando 97 del progetto di decisione, l'IPAA 2024 ha apportato solo modifiche limitate, in particolare attraverso l'introduzione di vice IPC ai quali l'IPC può delegare poteri specifici quando non sono in grado o non sono disponibili a svolgere le loro funzioni. Tali vice IPC devono essere commissari giudiziari e sono nominati dall'IPC.
95. L'EDPB osserva con soddisfazione che sono state scartate le precedenti idee nell'ambito del progetto di legge DPDI, che ha preceduto la DUUA, di abolire il Biometrics and Surveillance Camera Commissioner e di trasferire il ruolo all'Investigatory Powers Commissioner ⁽⁷⁷⁾. A tale riguardo, l'EDPB invita la Commissione a prestare ulteriore attenzione e a fornire una valutazione più dettagliata del ruolo del Biometrics and Surveillance Camera Commissioner nel sistema di vigilanza durante il suo monitoraggio e i futuri riesami del progetto di decisione.
96. Come già sottolineato dall'EDPB nel parere 14/2021, sebbene l'ICO sia adeguatamente dotato dei poteri necessari, che corrispondono in gran parte ai poteri delle autorità di controllo degli Stati membri dell'UE di cui all'articolo 58 del RGPD, l'esistenza di sanzioni efficaci svolge un ruolo importante nel garantire il rispetto delle regole ⁽⁷⁸⁾.
97. L'EDPB prende atto con soddisfazione della politica di trasparenza dell'ICO e della disponibilità di dati statistici e analitici, compresi esempi, delle attività di contrasto dell'ICO nei confronti degli organismi di contrasto ⁽⁷⁹⁾. A tale riguardo, l'EDPB osserva una preferenza dell'autorità di controllo del Regno Unito per gli ammonimenti in caso di violazioni della legislazione in materia di protezione dei dati da parte delle forze di polizia. Un'eccezione degna di nota è costituita dall'avviso di esecuzione emesso nel gennaio 2024 nei confronti della Crown Prosecution Service ⁽⁸⁰⁾. L'EDPB ritiene inoltre positivo il fatto che l'ICO abbia pubblicato numerosi codici di pratiche, linee guida, pareri e altri documenti di orientamento per le parti interessate.
98. Alla luce di quanto precede e in particolare in considerazione degli imminenti cambiamenti sostanziali della struttura e dell'organizzazione dell'autorità di controllo del Regno Unito, come già analizzato al punto 68 del presente parere, l'EDPB invita la Commissione europea a continuare a monitorare l'efficacia delle sanzioni e dei relativi mezzi di ricorso nel quadro sulla protezione dei dati del Regno Unito.

⁽⁷⁷⁾ Cfr <https://www.gov.uk/government/organisations/biometrics-and-surveillance-camera-commissioner>.

⁽⁷⁸⁾ Cfr. il parere 14/2021 dell'EDPB, punto 112.

⁽⁷⁹⁾ Cfr. ad esempio le serie di dati dettagliate sui reclami relativi alla protezione dei dati disponibili all'indirizzo <https://ico.org.uk/action-weve-taken/complaints-and-concerns-data-sets/data-protection-complaints/>.

⁽⁸⁰⁾ Cfr <https://ico.org.uk/action-weve-taken/enforcement/crown-prosecution-service-1/>.

4.2. ACCESSO E USO DA PARTE DELLE AUTORITÀ PUBBLICHE DEL REGNO UNITO A FINI DI SICUREZZA NAZIONALE

99. Il progetto di decisione offre solo dettagli limitati sull'accesso ai dati personali e sul loro utilizzo da parte delle autorità pubbliche del Regno Unito a fini di sicurezza nazionale. La Commissione spiega che la DUAA ha apportato solo modifiche minori al quadro che disciplina il trattamento dei dati da parte dei servizi di intelligence del Regno Unito ⁽⁸¹⁾, alcune delle quali sono state introdotte anche nel regime di contrasto della DPA 2018. Tali modifiche sono brevemente menzionate nel considerando 75 del progetto di decisione. Inoltre, le modifiche apportate all'IPA 2016 dopo l'adozione della precedente decisione di adeguatezza del Regno Unito sono già trattate nell'articolo 3.2 del progetto di decisione, in cui riguardano il trattamento dei dati a fini sia di contrasto sia di sicurezza nazionale ⁽⁸²⁾. Di conseguenza, le richieste di chiarimento e monitoraggio di cui alle precedenti sezioni 4.1.1.1 e 4.1.3 si applicano anche all'accesso e all'uso dei dati personali a fini di sicurezza nazionale.

4.2.1. UTILIZZO DEGLI AVVISI DI CAPACITÀ TECNICHE

100. All'inizio di quest'anno le relazioni dei media hanno rivelato che il governo del Regno Unito aveva presumibilmente emesso un avviso di capacità tecniche ai sensi dell'articolo 253 dell'IPA 2016 a un'importante società tecnologica, richiedendo al fornitore di poter mantenere l'accesso ai dati criptati dei suoi utenti in forma decriptata ⁽⁸³⁾. In pratica, presumibilmente, ciò significherebbe eludere la cifratura end-to-end offerta dal fornitore per la sua soluzione di archiviazione su cloud. Questa misura è stata pertanto definita una «domanda backdoor».
101. Sebbene la base giuridica per gli avvisi di capacità tecniche esistesse già al momento dell'adozione della precedente decisione di adeguatezza del Regno Unito, questo caso segnalato sembra segnare la prima istanza nota di una domanda di questo tipo. In quanto tale, si tratta di uno sviluppo significativo che merita attenzione, in particolare alla luce dell'articolo 45, paragrafo 2, lettera a), del RGPD, che richiede una valutazione non solo del quadro giuridico sulla carta, ma anche della sua attuazione ⁽⁸⁴⁾. L'EDPB si sarebbe pertanto aspettato che il progetto di decisione affrontasse esplicitamente la questione e incoraggia la Commissione a integrare di conseguenza la decisione.
102. Nonostante il fatto che i dettagli del caso di specie non siano pienamente noti al pubblico a causa della natura riservata degli avvisi di capacità tecniche, dall'elenco pubblico della domanda di udienza in privato sul sito web dell'Investigatory Powers Tribunal, nonché dall'estratto pubblicamente disponibile della sentenza privata relativa a tale udienza, risulta che non si tratta di una questione di speculazione mediatica ⁽⁸⁵⁾. La questione giustifica la menzione e la presunta applicazione dell'articolo 253 dell'IPA 2016 per l'emissione di una «domanda backdoor» deve essere segnalata per un monitoraggio futuro.
103. Come recentemente sottolineato nella dichiarazione 05/2024, l'EDPB ritiene che la cifratura sia essenziale per garantire la sicurezza e la riservatezza dei dati personali e delle comunicazioni elettroniche. In particolare, l'autentica cifratura end-to-end che riguarda i dispositivi terminali e i dati

⁽⁸¹⁾ Cfr. il considerando 75 del progetto di decisione.

⁽⁸²⁾ Cfr. il considerando 98 del progetto di decisione. I poteri di indagine in questione possono essere esercitati non solo dalle agenzie di intelligence nazionali, ma anche da talune autorità di contrasto.

⁽⁸³⁾ Cfr. «U.K. orders Apple to let it spy on users' encrypted accounts» (Washington Post, 7 febbraio 2025), <https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/>.

⁽⁸⁴⁾ Inoltre, l'articolo 45, paragrafo 3, del RGPD, specifica che la Commissione tiene conto di tutti gli sviluppi pertinenti nel paese terzo quando riesamina periodicamente le sue constatazioni di adeguatezza.

⁽⁸⁵⁾ Cfr. <https://www.judiciary.uk/judgments/apple-inc-v-secretary-of-state-for-the-home-department/>.

in essi contenuti, con le chiavi di decifratura in possesso esclusivamente dell'utente, è uno strumento fondamentale per garantire la riservatezza delle comunicazioni elettroniche ⁽⁸⁶⁾. Gli avvisi di capacità tecniche che obbligano le imprese a fornire la capacità di rimuovere la cifratura su richiesta del governo creano vulnerabilità sistemiche e rappresentano una minaccia diretta all'integrità e alla riservatezza delle comunicazioni elettroniche. A tale riguardo, l'EDPB richiama l'attenzione sulla causa PODCHASOV/RUSSIA, in cui la Corte europea dei diritti dell'uomo ha rilevato che l'obbligo di decifrare le comunicazioni cifrate end-to-end comporta l'obbligo per i fornitori di tali servizi di indebolire il meccanismo di cifratura per tutti gli utenti; esso non è pertanto proporzionato agli obiettivi legittimi perseguiti ⁽⁸⁷⁾.

104. Pur supponendo che il governo del Regno Unito cercherebbe principalmente di accedere ai dati degli utenti senza cifratura in caso di rischio per la sicurezza nazionale, l'EDPB ritiene che la richiesta di valutazione dell'uso degli avvisi di capacità tecniche, come discusso in precedenza, sia ugualmente pertinente nel contesto dell'accesso da parte di pubbliche amministrazioni a fini di contrasto.

4.2.2. BASI GIURIDICHE E GARANZIE APPLICABILI

105. L'IPAA 2024 ha introdotto un regime specifico per la conservazione e l'esame di serie massive di dati personali per i quali le persone cui si riferiscono i dati personali non potrebbero avere solo una scarsa o nessuna ragionevole aspettativa di tutela della vita privata, come stabilito dalla legge ⁽⁸⁸⁾. Per la conservazione e l'esame di tale sottoinsieme specifico di serie massive di dati personali, l'IPA 2016 prevede ora la possibilità di «autorizzazioni individuali» e «autorizzazioni per categoria».⁸⁹
106. La nozione di serie massive di dati personali è ampia e può rilevare una vasta gamma di serie di dati ⁽⁹⁰⁾. Può applicarsi a informazioni sensibili, ma può comprendere anche dati disponibili al pubblico e in commercio. In tale contesto, il governo del Regno Unito ha ritenuto necessario rivedere il regime precedente che applicava lo stesso livello di garanzie a tutte le serie massive di dati personali e prevedere, invece, garanzie diverse per la conservazione e l'esame delle serie massive di dati personali, a seconda della sensibilità o della disponibilità pubblica dei loro contenuti, o del livello di intrusione associato ai servizi di intelligence che li conservano e li esaminano ⁽⁹¹⁾. È opinione dell'EDPB che queste considerazioni abbiano in ultima analisi portato alla creazione di un regime distinto per le serie massive di dati personali in cui vi è solo una scarsa o nessuna ragionevole aspettativa di tutela della vita privata.
107. Mentre la Commissione discute brevemente il nuovo concetto di «autorizzazione per categoria», il progetto di decisione afferma che soprattutto, per la conservazione e l'esame delle serie massive di dati personali, rimane in vigore il regime valutato nei considerando 239 e 240 della decisione di

⁽⁸⁶⁾ Cfr. la dichiarazione 5/2024 sulle raccomandazioni del gruppo di alto livello sull'accesso ai dati per un contrasto efficace, adottata il 4 novembre 2024, pagg. 4 e 5.

⁽⁸⁷⁾ Cfr. la sentenza della Corte europea dei diritti dell'uomo del 13 febbraio 2024, 33696/19, punto 79.

⁽⁸⁸⁾ Cfr. l'articolo 226 A, paragrafo 1, dell'IPA 2016.

⁽⁸⁹⁾ Cfr. gli articoli 226 A e 226 BA dell'IPA 2016, introdotti dall'articolo 2 dall'Investigatory Powers Amendment Act del 2024.

⁽⁹⁰⁾ Cfr. l'articolo 199 dell'IPA 2016 che specifica che un servizio di intelligence conserva una serie massiva di dati personali se a) il servizio di intelligence ottiene una serie di informazioni che comprendono dati personali relativi a un certo numero di persone, b) la natura della serie è tale che la maggior parte delle persone non è, e probabilmente non diventerà, di interesse per il servizio di intelligence nell'esercizio delle sue funzioni, c) dopo qualsiasi esame iniziale dei contenuti, il servizio di intelligence conserva la serie ai fini dell'esercizio delle sue funzioni e d) la serie è detenuta, o deve essere detenuta, elettronicamente per l'analisi nell'esercizio di tali funzioni.

⁽⁹¹⁾ Cfr. Home Office, Policy paper Investigatory Powers (Amendment) Bill: Bulk Personal Datasets and Third Party Bulk Personal Datasets, <https://www.gov.uk/government/publications/investigatory-powers-amendment-bill-factsheets/investigatory-powers-amendment-bill-bulk-personal-datasets-and-third-party-bulk-personal-datasets>.

esecuzione (UE) 2021/1772, in particolare la necessità di un mandato approvato prima dal segretario di Stato e poi dal commissario giudiziario, nel rispetto dei requisiti di necessità e proporzionalità della misura, come previsto dalla parte 7 dell'IPA 2016» ⁽⁹²⁾. Tuttavia, tale analisi sembra essere incompleta. L'EDPB osserva che non solo l'introduzione di «autorizzazioni per categoria», ma anche di «autorizzazioni individuali» costituisce una modifica pertinente attuata dall'IPAA 2024 per quanto riguarda la serie specifica di dati di cui sopra: una «autorizzazione individuale», che può essere concessa dal capo di un servizio di intelligence, o da una persona che agisce per suo conto, sostituisce la necessità di ottenere un mandato al fine di conservare, o conservare ed esaminare, serie massive di dati personali per le quali vi è solo una scarsa o nessuna ragionevole aspettativa di tutela della vita privata ⁽⁹³⁾. I termini «mandato» e «autorizzazione individuale» non dovrebbero pertanto essere confusi e non possono essere utilizzati in modo intercambiabile ⁽⁹⁴⁾. Ciò è dovuto in particolare al fatto che l'approvazione giudiziaria richiesta per le singole autorizzazioni è limitata alla questione se la serie di dati specifica soddisfi i criteri per essere classificata come tale da giustificare solo una scarsa o nessuna ragionevole aspettativa di tutela della vita privata ai sensi dell'articolo 226 A dell'IPA 2016 ⁽⁹⁵⁾. Un'«autorizzazione per categoria» è diversa da un'«autorizzazione individuale» e non applica di fatto – per la l'articolo 226B, paragrafo 6, lettera a), dell'IPA 2016 – il requisito dell'approvazione giudiziaria di un'autorizzazione individuale, laddove tale autorizzazione riguardi una serie di dati che rientra in un'autorizzazione per categoria. Ciò è dovuto al fatto che una decisione sarà già stata presa, e approvata da un commissario giudiziario, in base alla quale qualsiasi serie di dati che rientri nella descrizione nell'autorizzazione per categoria è in effetti una serie di dati alla quale si applicherebbe l'articolo 226 A.

108. Sebbene tali modifiche riguardino la conservazione e l'esame di serie massive di dati personali e non la loro intercettazione o raccolta iniziale, l'EDPB desidera sottolineare l'importanza che la Corte europea dei diritti dell'uomo attribuisce alla previa autorizzazione indipendente nel contesto del trattamento massivo di dati personali. La Corte ha stabilito che al fine di ridurre al minimo il rischio di abuso del potere di intercettazione massiva, il processo deve essere soggetto a «garanzie end-to-end», il che significa che, a livello nazionale, si dovrebbe effettuare una valutazione in ogni fase del processo della necessità e della proporzionalità delle misure adottate; che l'intercettazione massiva dovrebbe essere soggetta a un'autorizzazione indipendente fin dall'inizio, quando l'oggetto e la portata dell'operazione sono definiti; e che l'operazione dovrebbe essere soggetta a un controllo e a un riesame *ex post* indipendente ⁽⁹⁶⁾. In quest'ottica e sulla base di un approccio olistico, che tenga conto di tutte le circostanze del caso nel valutare l'adeguatezza, l'EDPB ritiene che la conservazione e l'esame delle serie massive di dati personali debbano essere almeno soggetti a un'autorizzazione preventiva da parte di un'autorità indipendente o a un riesame sistematico indipendente *ex post* da parte di un giudice o di un organismo equivalente, vale a dire un organismo indipendente che può rendere decisioni vincolanti.
109. Alla luce dei restanti chiarimenti necessari, l'EDPB esorta la Commissione a esaminare ulteriormente i concetti di «autorizzazioni individuali» e di «autorizzazioni per categoria» ai sensi dell'IPAA 2024. Inoltre, l'EDPB invita la Commissione a monitorare attentamente l'attuazione nella pratica

⁽⁹²⁾ Cfr. il considerando 99 del progetto di decisione.

⁽⁹³⁾ Articolo 200, paragrafi 1 e 2, dell'IPA 2016.

⁽⁹⁴⁾ Ciò sembra tuttavia verificarsi nei considerando 99 e 100 del progetto di decisione.

⁽⁹⁵⁾ L'articolo 226 BB, paragrafo 1, dell'IPA 2016 stabilisce che, nel decidere se approvare una decisione di rilascio di un'autorizzazione individuale o di un'autorizzazione per categoria, un commissario giudiziario deve riesaminare le conclusioni della persona che ha concesso l'autorizzazione per verificare se l'articolo 226 A si applichi alla serie massiva di dati personali descritto nell'autorizzazione o, rispettivamente, se l'articolo 226 A si applichi a qualsiasi serie di dati che rientra nella categoria di serie di dati descritta nell'autorizzazione.

⁽⁹⁶⁾ CEDU, *Big Brother Watch e a./Regno Unito*, 25 maggio 2021, punto 350.

dell'espressione «scarsa o nessuna ragionevole aspettativa di tutela della vita privata». Sebbene l'articolo 226 A dell'IPA 2016 stabilisca una serie di criteri per tale constatazione, l'EDPB ritiene importante osservarne l'applicazione, in quanto potenzialmente soggetti a un'interpretazione estensiva ⁽⁹⁷⁾.

4.2.3. VIGILANZA E RICORSO

110. Come indicato nel progetto di decisione e precedentemente analizzato nel parere 14/2021, l'Investigatory Powers Commissioner (IPC) e il suo ufficio (IPCO) svolgono un ruolo centrale nella sorveglianza dell'uso dei poteri di indagine da parte delle agenzie di intelligence del Regno Unito. Inoltre, l'Investigatory Powers Tribunal (organo giurisdizionale competente per i poteri di indagine) è l'organo giudiziario che fornisce i mezzi di ricorso al riguardo. Come già indicato nell'articolo 3.1.5 sulla vigilanza nell'ambito delle attività di contrasto, l'IPAA 2024 ha apportato solo modifiche limitate, in particolare attraverso l'introduzione dei vice IPC. Pertanto, le osservazioni dell'EDPB nel suo parere 14/2021 restano pienamente valide ⁽⁹⁸⁾.
111. L'EDPB prende atto con soddisfazione della trasparenza delle relazioni annuali dell'IPCO, compresa la disponibilità di statistiche dettagliate per il periodo 2019-2023, anche in merito all'uso in maniera massiva di poteri da parte della comunità di intelligence del Regno Unito e alle decisioni di scelta dell'obiettivo e alle autorizzazioni mirate ai fini dell'acquisizione di dati ai sensi dell'accordo tra Regno Unito e Stati Uniti sull'accesso ai dati. L'EDPB prende inoltre atto specificamente delle attività di sorveglianza dell'IPCO sull'intercettazione massiva di dati da parte del Government Communications Headquarters, evidenziate dalla Commissione al considerando 102 del progetto di decisione. In tale contesto, l'EDPB invita la Commissione a continuare a monitorare attentamente l'efficacia del sistema di vigilanza in questo settore, in particolare per quanto riguarda la proporzionalità delle richieste di intercettazione massiva ⁽⁹⁹⁾.
112. Inoltre, l'EDPB osserva che l'Investigatory Powers Tribunal ha pubblicato anche una relazione pubblica sulle sue attività e sulla sua giurisprudenza per il periodo 2021-2023 ⁽¹⁰⁰⁾. La relazione evidenzia, tra l'altro, sviluppi importanti e pertinenti come la sentenza della CEDU nella causa *Wieder e Guarnieri/Regno Unito*, che ha stabilito che le persone di qualsiasi parte del mondo possono presentare una richiesta di risarcimento all'Investigatory Powers Tribunal, se la condotta riguarda un organismo pubblico del Regno Unito e se il fatto si è verificato nel Regno Unito. L'EDPB invita pertanto la Commissione a includere anche le attività dell'Investigatory Powers Tribunal nella sua valutazione e nei futuri riesami del progetto di decisione.

5. RIESAME, DURATA E RINNOVO DEL PROGETTO DI DECISIONE

113. L'EDPB osserva che la decisione di adeguatezza finale si applicherebbe per sei anni, ossia fino al 27 dicembre 2031. Continuerebbe quindi a essere l'unico paese terzo la cui decisione di adeguatezza prevede una clausola di caducità combinata con il riesame periodico obbligatorio di cui all'articolo 45,

⁽⁹⁷⁾ L'articolo 226 A dell'IPA 2016 fa riferimento, ad esempio, alla natura dei dati, alla misura in cui i dati sono stati resi pubblici o alla misura in cui i dati sono ampiamente noti.

⁽⁹⁸⁾ Cfr. il parere 14/2021, punti da 200 a 215.

⁽⁹⁹⁾ Per maggiori informazioni, cfr. la relazione annuale 2023 dell'IPC, disponibile al seguente indirizzo: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf, pag. 31, punto 6.41.

⁽¹⁰⁰⁾ <https://investatorypowertribunal.org.uk/wp-content/uploads/2024/11/Investigatory-Powers-Tribunal-Report-2024.pdf>

paragrafo 3, del RGPD. L'EDPB è consapevole del fatto che il nuovo quadro giuridico del Regno Unito meriterà un'attenzione specifica e invita la Commissione a monitorare attentamente l'attuazione della DUAA, compresi i settori di interesse evidenziati nel presente parere, nonché tutti gli altri sviluppi pertinenti nel Regno Unito a tale riguardo.

114. L'EDPB accoglie con favore il fatto che il considerando 68 del progetto di decisione faccia riferimento al ruolo dell'EDPB (e dei gruppi della società civile) nel meccanismo di riesame periodico, conformemente alla raccomandazione 01/2021 dell'EDPB ⁽¹⁰¹⁾. Per quanto riguarda il coinvolgimento pratico dell'EDPB e dei suoi rappresentanti nella preparazione e nello svolgimento del futuro riesame, l'EDPB ribadisce che qualsiasi documentazione pertinente dovrebbe essere condivisa per iscritto con l'EDPB con sufficiente anticipo.
115. Dalle spiegazioni aggiuntive fornite dalla Commissione in relazione al considerando 113, l'EDPB comprende che l'intenzione è quella di effettuare un riesame al termine dei quattro anni sulla base dei quali la Commissione preparerà una relazione pubblica ⁽¹⁰²⁾. Tale riesame contribuirà a informare la Commissione se, al più tardi sei mesi prima della fine del progetto di decisione, avvierà la procedura per prorogare la durata del progetto di decisione ⁽¹⁰³⁾.
116. L'EDPB accoglie con favore tale intenzione e osserva che, poiché il riesame ha una finalità diversa dalla clausola di caducità e svolge un ruolo importante nel monitoraggio del quadro giuridico. L'EDPB, pertanto, si aspetta che il riesame si svolga entro quattro anni e incoraggia la Commissione a procedere in tal senso a tempo debito.
117. L'EDPB capisce che questo futuro riesame terrà conto degli elementi delineati nella decisione di esecuzione (UE) 2021/1772 della Commissione e che i considerando relativi alla sospensione e all'abrogazione della decisione sono ancora validi ⁽¹⁰⁴⁾. Ai fini della certezza del diritto, l'EDPB ritiene che tale chiarimento possa comparire nella decisione di adeguatezza finale.

Per il comitato europeo per la protezione dei dati

La presidente

(Anu Talus)

⁽¹⁰¹⁾ Cfr. il considerando 19 della raccomandazione 01/2021 dell'EDPB.

⁽¹⁰²⁾ Cfr. il considerando 110 del progetto di decisione.

⁽¹⁰³⁾ Cfr. il considerando 113 del progetto di decisione.

⁽¹⁰⁴⁾ Cfr. i considerando da 168 a 171 della decisione di esecuzione 2021/1173 della Commissione.