



**DECISIONE DI ESECUZIONE (UE) 2025/2571 DELLA COMMISSIONE
del 19 dicembre 2025**

che modifica la decisione di esecuzione (UE) 2021/1773 della Commissione a norma della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte del Regno Unito

[notificata con il numero C(2025) 8782]

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

vista la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie)⁽¹⁾, in particolare l'articolo 36, paragrafo 3,

considerando quanto segue:

1. INTRODUZIONE

- (1) La decisione di esecuzione (UE) 2021/1773 della Commissione⁽²⁾ conclude che, ai fini dell'articolo 36 della direttiva (UE) 2016/680, il Regno Unito assicura un livello di protezione adeguato dei dati personali trasferiti nell'ambito di applicazione di tale direttiva dall'Unione europea verso il Regno Unito.
- (2) Nell'adottare la decisione di esecuzione (UE) 2021/1773, la Commissione ha tenuto conto del fatto che, alla fine del periodo di transizione previsto dall'accordo sul recesso del Regno Unito di Gran Bretagna e Irlanda del Nord dall'Unione europea e dalla Comunità europea dell'energia atomica⁽³⁾ e non appena la disposizione provvisoria di cui all'articolo 782 dell'accordo sugli scambi commerciali e la cooperazione tra l'Unione europea e la Comunità europea dell'energia atomica, da una parte, e il Regno Unito di Gran Bretagna e Irlanda del Nord, dall'altra⁽⁴⁾ avesse cessato di applicarsi, il Regno Unito avrebbe adottato, applicato e fatto rispettare un nuovo regime di protezione dei dati, diverso da quello in vigore quando era vincolato dal diritto dell'Unione.
- (3) Poiché ciò avrebbe potuto comportare modifiche del quadro in materia di protezione dei dati, valutato nella decisione di esecuzione (UE) 2021/1773, o altri importanti sviluppi, si è ritenuto opportuno prevedere che tale decisione si applicasse per un periodo di quattro anni a decorrere dalla sua entrata in vigore. Era stato perciò stabilito che la decisione di esecuzione (UE) 2021/1773 scadesse il 27 giugno 2025, a meno che non fosse prorogata secondo la procedura di cui all'articolo 58, paragrafo 2, della direttiva (UE) 2016/680.
- (4) Per decidere in merito a un'eventuale proroga della decisione di esecuzione (UE) 2021/1773, la Commissione deve valutare 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 suddetta decisione per quanto riguarda gli elementi di cui all'articolo 36, paragrafo 2, della direttiva (UE) 2016/680.
- (5) In particolare, il 23 ottobre 2024 il governo del Regno Unito ha presentato al parlamento del Regno Unito il disegno di legge sull'accesso ai dati e sul loro utilizzo [Data (Use and Access) Bill]⁽⁵⁾, proponendo modifiche della legge del 2018 sulla protezione dei dati (Data Protection Act 2018), valutata nella decisione di esecuzione

⁽¹⁾ GU L 119 del 4.5.2016, pag. 89, ELI: <http://data.europa.eu/eli/dir/2016/680/oj>.

⁽²⁾ Decisione di esecuzione (UE) 2021/1773 della Commissione, del 28 giugno 2021, a norma della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte del Regno Unito (GU L 360 dell'11.10.2021, pag. 69, ELI: http://data.europa.eu/eli/dec_impl/2021/1773/oj).

⁽³⁾ GU C 384I del 12.11.2019, pag. 1.

⁽⁴⁾ GU L 149 del 30.4.2021, pag. 10, ELI: [http://data.europa.eu/eli/agree_internation/2021/689\(1\)/oj](http://data.europa.eu/eli/agree_internation/2021/689(1)/oj).

⁽⁵⁾ Disponibile al seguente indirizzo: <https://bills.parliament.uk/bills/3825/news>.

(UE) 2021/1773. Il 24 giugno 2025 la Commissione ha adottato la decisione di esecuzione (UE) 2025/1225 della Commissione (⁶), che ha prorogato la validità della decisione (UE) 2021/1773 per un periodo di sei mesi fino al 27 dicembre 2025. Questa proroga tecnica limitata nel tempo ha consentito alla Commissione di completare la valutazione dell'adeguato livello di protezione dei dati personali fornito dal Regno Unito sulla base di un quadro giuridico stabile, ossia dopo la conclusione del pertinente processo legislativo.

- (6) Dall'adozione della decisione di esecuzione (UE) 2021/1773 la Commissione ha controllato su base continuativa gli sviluppi pertinenti nel Regno Unito (⁷). Conformemente al considerando 165 della decisione di esecuzione (UE) 2021/1773, è stata prestata particolare attenzione all'applicazione pratica delle norme del Regno Unito sul trasferimento di dati personali verso paesi terzi, all'impatto di tale applicazione sul livello di protezione offerto ai dati trasferiti a norma di detta decisione di esecuzione e all'effettività dell'esercizio dei diritti individuali, compresi eventuali sviluppi legislativi e pratici pertinenti riguardanti eccezioni o limitazioni di tali diritti. Assieme ad altri elementi, gli sviluppi giurisprudenziali e la vigilanza da parte dell'ufficio dell'Information Commissioner (ICO) e di altri organismi indipendenti hanno contribuito al monitoraggio della Commissione.
- (7) Sulla base della valutazione di tali sviluppi, comprese le modifiche della legge del 2018 sulla protezione dei dati introdotte dalla legge sull'accesso ai dati e sul loro utilizzo (Data (Use and Access) Act), la Commissione conclude che il Regno Unito continua ad assicurare un livello di protezione adeguato dei dati personali trasferiti dall'Unione europea verso il Regno Unito nell'ambito di applicazione della direttiva (UE) 2016/680.

2. IMPORTANTI SVILUPPI RIGUARDANTI LE NORME CHE SI APPLICANO AL TRATTAMENTO DI DATI PERSONALI

2.1. Quadro del Regno Unito in materia di protezione dei dati

- (8) All'epoca dell'adozione della decisione di esecuzione (UE) 2021/1773, il quadro giuridico riguardante il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica, nel Regno Unito era definito nelle parti pertinenti dalla legge del 2018 sulla protezione dei dati (⁸), come modificata dai Data Protection, Privacy and Electronic Communications (Amendments ecc.) (EU Exit) Regulations 2019 (regolamenti DPPEC) (⁹), in particolare nella parte 3 di tale legge.
- (9) Sebbene tale legge, che rispecchiava in larga misura le corrispondenti norme applicabili all'interno dell'Unione europea, continui a costituire la legislazione del Regno Unito in materia di protezione dei dati per le pertinenti attività di trattamento, da allora è stata oggetto di alcune modifiche limitate, che riflettono il fatto che il Regno Unito non è più soggetto al diritto dell'Unione europea.
- (10) In primo luogo, la legge del 2023 sul diritto dell'Unione mantenuto (revoca e riforma) [Retained EU Law (Revocation and Reform) Act 2023] (¹⁰) ha chiarito che i principi generali del diritto dell'UE non rientrano più nel diritto interno del Regno Unito dalla fine del 2023 (¹¹). Inoltre gli organi giurisdizionali del Regno Unito non sono più tenuti a interpretare il «diritto assimilato» non modificato, precedentemente denominato «diritto dell'Unione mantenuto», in

(⁶) Decisione di esecuzione (UE) 2025/1225 della Commissione, del 24 giugno 2025, che modifica la decisione di esecuzione (UE) 2021/1773 a norma della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte del Regno Unito (GU L, 2025/1225, 26.6.2025, ELI: http://data.europa.eu/eli/dec_impl/2025/1225/oj).

(⁷) Articolo 36, paragrafo 4, della direttiva (UE) 2016/680.

(⁸) Legge del 2018 sulla protezione dei dati, disponibile al seguente indirizzo: <https://www.legislation.gov.uk/ukpga/2018/12/contents>. Prima del recesso del Regno Unito dall'Unione europea e durante il periodo di transizione, la legge del 2018 sulla protezione dei dati prevedeva norme nazionali, ove consentito dal regolamento (UE) 2016/679, che specificavano e limitavano l'applicazione delle norme del regolamento (UE) 2016/679, e recepiva la direttiva (UE) 2016/680.

(⁹) The Data Protection, Privacy and Electronic Communications (Amendments ecc.) (EU Exit) Regulations 2019 [(regolamenti del 2019 in materia di protezione dei dati, tutela della vita privata e comunicazioni elettroniche (modifiche ecc.) (Uscita dall'UE)], disponibili al seguente indirizzo: <https://www.legislation.gov.uk/uksi/2019/419/contents/made>, come modificati dai regolamenti DPPEC 2020, disponibili al seguente indirizzo: <https://www.legislation.gov.uk/ukdsi/2020/9780348213522>. I regolamenti DPPEC modificano il regolamento (UE) 2016/679 come recepito nel diritto del Regno Unito attraverso la legge del 2018 relativa al recesso dall'Unione europea, la legge del 2018 sulla protezione dei dati e altra legislazione in materia di protezione dei dati, al fine di adattarlo al contesto interno.

(¹⁰) Legge del 2023 sul diritto dell'Unione mantenuto (revoca e riforma), disponibile al seguente indirizzo: <https://www.legislation.gov.uk/ukpga/2023/28>.

(¹¹) Sezione 5 della legge del 2018 relativa al recesso dall'Unione europea, come modificata dalla legge sul diritto dell'Unione mantenuto (revoca e riforma).

modo conforme ai principi generali del diritto dell'Unione, in quanto tale diritto deve essere invece interpretato in modo compatibile con il diritto interno del Regno Unito⁽¹²⁾. Tuttavia gli organi giurisdizionali del Regno Unito devono interpretare il diritto assimilato non modificato conformemente alla pertinente giurisprudenza della Corte di giustizia dell'Unione europea emessa prima della fine del periodo di transizione⁽¹³⁾, come indicato anche nel considerando 12 della decisione di esecuzione (UE) 2021/1773. La legge del 2018 sulla protezione dei dati è stata modificata dalla legge sull'accesso ai dati e sul loro utilizzo per chiarire l'effetto della legge sul diritto dell'Unione mantenuto (revoca e riforma) sulla legislazione del Regno Unito in materia di protezione dei dati. Ad esempio, la sezione 183 A, paragrafo 1, della legge del 2018 sulla protezione dei dati prevede, come regola generale, che qualsiasi nuova normativa (adottata il 20 agosto 2025 o successivamente) che introduce nuovi obblighi o poteri ai fini del trattamento dei dati personali sia considerata soggetta alla legislazione del Regno Unito in materia di protezione dei dati. Ciò significa che il quadro in materia di protezione dei dati del Regno Unito continua a prevalere su altre normative. Ai sensi della sezione 183 A, paragrafo 2, lettera b), della legge del 2018 sulla protezione dei dati, tale presunzione può essere disapplicata se il parlamento del Regno Unito decide deliberatamente di farlo in modo espresso nella legislazione, preservando la sovranità parlamentare. Inoltre la sezione 186, paragrafo 2 A, della legge del 2018 sulla protezione dei dati chiarisce che sulle limitazioni ai diritti degli interessati di cui alla sezione 186, paragrafo 3, della legge del 2018 non prevale la sezione 186, paragrafo 1, della medesima legge, che prevede che le disposizioni che vietano o limitano la divulgazione di informazioni non prevalgano su determinati diritti in materia di protezione dei dati. Ciò garantisce che, ad esempio, le limitazioni dei diritti degli interessati stabilite nella legge del 2018 sulla protezione dei dati non rientrino di per sé nella «prevalenza della protezione dei dati» di cui alla sezione 186, paragrafo 1, della legge del 2018.

- (11) In secondo luogo, dall'adozione della decisione di esecuzione (UE) 2021/1773, la legislazione del Regno Unito in materia di protezione dei dati è stata modificata mediante i regolamenti di modifica del 2023 sulla protezione dei dati (diritti e libertà fondamentali) (Data Protection (Fundamental Rights and Freedoms) Amendment Regulations 2023)⁽¹⁴⁾. Tali regolamenti definiscono i riferimenti ai diritti e alle libertà fondamentali nella legge del 2018 sulla protezione dei dati (precedentemente definiti in modo da includere i diritti e le libertà fondamentali dell'UE⁽¹⁵⁾) come riferimenti ai diritti sanciti dalla convenzione europea dei diritti dell'uomo, che sono stati attuati nel diritto interno del Regno Unito ai sensi della legge del 1998 sui diritti umani (Human Rights Act 1998)⁽¹⁶⁾. La legge del 1998 sui diritti umani integra nel diritto del Regno Unito i diritti sanciti dalla convenzione europea dei diritti dell'uomo. Tale legge accorda a qualsiasi persona fisica i diritti e le libertà fondamentali di cui agli articoli da 2 a 12 e 14 della convenzione europea dei diritti dell'uomo, agli articoli 1, 2 e 3 del suo primo protocollo e all'articolo 1 del suo tredicesimo protocollo, in combinato disposto con gli articoli 16, 17 e 18 della convenzione medesima. Tra di essi è compreso il diritto al rispetto della vita privata e familiare (così come la protezione dei dati personali rientrante in tale diritto) e il diritto a un equo processo⁽¹⁷⁾.
- (12) In ultimo luogo, la legge del 2018 sulla protezione dei dati è stata oggetto di riforme mirate previste dalle parti 5 e 6 della legge sull'accesso ai dati e sul loro utilizzo. Sebbene il suo ambito di applicazione vada ben oltre la protezione dei dati personali, la legge sull'accesso ai dati e sul loro utilizzo prevede limitate modifiche di diversi aspetti del regime di protezione dei dati, quali, tra l'altro, le modalità di esercizio dei diritti degli interessati, le condizioni per il processo decisionale automatizzato e l'ambito di applicazione di determinati obblighi in materia di responsabilità. Inoltre la legge sull'accesso ai dati e sul loro utilizzo apporta modifiche alla struttura di governance dell'ICO. Una volta attuate, queste misure sostituiranno l'ICO con una nuova entità, la Information Commission. Il ruolo e le funzioni dell'autorità di regolamentazione in qualità di autorità indipendente di controllo della protezione dei dati nel Regno Unito rimarranno invariati. La legge introduce anche nuovi poteri di esecuzione per l'autorità di regolamentazione.
- (13) La presente decisione valuta gli sviluppi legislativi, normativi e di altro tipo attinenti alle conclusioni sul livello di protezione garantita dal Regno Unito, formulate nella decisione di esecuzione (UE) 2021/1773. La valutazione effettuata nella decisione di esecuzione (UE) 2021/1773 rimane valida per quanto riguarda gli aspetti del quadro in materia di protezione dei dati del Regno Unito che non sono stati modificati o influenzati da altri sviluppi successivi all'adozione della decisione di esecuzione (UE) 2021/1773.

⁽¹²⁾ Sezione 5, paragrafo A2, della legge del 2018 relativa al recesso dall'Unione europea, come modificata dalla legge sul diritto dell'Unione mantenuto (revoca e riforma).

⁽¹³⁾ Sezione 6, paragrafi 3 e 7, della legge del 2018 relativa al recesso dall'Unione europea, come modificata dalla legge sul diritto dell'UE mantenuto (revoca e riforma).

⁽¹⁴⁾ Disponibili al seguente indirizzo: <https://www.gov.uk/government/publications/the-data-protection-fundamental-rights-and-freedoms-amendment-regulations-2023>.

⁽¹⁵⁾ I diritti e le libertà fondamentali dell'UE sono stati mantenuti nel diritto del Regno Unito mediante la sezione 4 della legge del 2018 relativa al recesso dall'Unione europea, abrogata alla fine del 2023 dalla legge sul diritto dell'UE mantenuto (revoca e riforma).

⁽¹⁶⁾ Sezione 2, paragrafo 3, dei regolamenti di modifica del 2023 sulla protezione dei dati (diritti e libertà fondamentali).

⁽¹⁷⁾ Articoli 6, 8, 10 e 13 CEDU (cfr. anche l'allegato 1 della legge del 1998 sui diritti umani, disponibile al seguente indirizzo: <https://www.legislation.gov.uk/ukpga/1998/42/contents>).

- (14) Gli sviluppi legislativi, normativi e altri sviluppi importanti sono analizzati in dettaglio nelle sezioni seguenti sulla base del livello di adeguatezza: la Commissione deve determinare se il paese terzo in questione garantisce un livello di protezione «sostanzialmente equivalente» a quello assicurato all'interno dell'Unione europea ⁽¹⁸⁾. Come chiarito dalla Corte di giustizia dell'Unione europea, non è richiesto un livello di protezione identico ⁽¹⁹⁾. In particolare, gli strumenti dei quali il paese terzo in questione si avvale per proteggere i dati personali possono essere diversi da quelli attuati all'interno dell'Unione europea, purché si rivelino efficaci, nella prassi, al fine di assicurare un livello adeguato di protezione ⁽²⁰⁾. Il livello di adeguatezza non comporta pertanto una duplicazione pedissequa delle norme dell'Unione. La prova consiste, piuttosto, nel determinare se, con la sostanza dei diritti alla protezione dei dati e rendendone l'attuazione, l'azionabilità e il controllo effettivi, il sistema giuridico estero, nel suo insieme, offre il necessario livello di protezione ⁽²¹⁾.

2.1.1. *Definizioni*

- (15) Nel regime di protezione dei dati del Regno Unito continuano ad applicarsi i concetti fondamentali di protezione dei dati che rispecchiano la terminologia della direttiva (UE) 2016/680. Tali concetti sono stati valutati nei considerando 26 e 27 della decisione di esecuzione (UE) 2021/1773.
- (16) In particolare, specificando la definizione e le condizioni per ottenere il consenso, la legge sull'accesso ai dati e sul loro utilizzo conferma il quadro giuridico che disciplina l'uso del consenso come base legittima per il trattamento dei dati personali ⁽²²⁾. Le disposizioni aggiornate riproducono la formulazione del GDPR del Regno Unito, aumentando in tal modo la coerenza tra i regimi di protezione dei dati del Regno Unito. Tale allineamento permette un'interpretazione più chiara da parte delle autorità competenti quando il consenso è invocato come base legittima per il trattamento.
- (17) In primo luogo, la sezione 69 della legge sull'accesso ai dati e sul loro utilizzo introduce nella legge del 2018 sulla protezione dei dati una nuova sottosezione 33, paragrafo 1 A, che definisce il termine «consenso» come una manifestazione dell'intenzione dell'interessato liberamente espressa, specifica, informata e inequivocabile. Tale intenzione deve essere manifestata mediante una dichiarazione o un atto positivo inequivocabile e deve esprimere l'accettazione dell'interessato al trattamento dei suoi dati personali.
- (18) In secondo luogo, la stessa sezione aggiunge alla legge del 2018 sulla protezione dei dati la sezione 40 A, che stabilisce le condizioni che devono essere soddisfatte allorché ci si basa sul consenso. Il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha manifestato un consenso valido. Se è ottenuto per iscritto all'interno di un documento più ampio, il consenso deve essere presentato in modo tale da poterlo distinguere chiaramente dalle altre materie, utilizzando un linguaggio semplice, comprensibile e accessibile. Qualsiasi disposizione del documento che non rispetti tali norme non è vincolante ⁽²³⁾.
- (19) I titolari del trattamento o i responsabili del trattamento devono inoltre informare l'interessato, prima che manifesti il consenso, del suo diritto di revocarlo. Revocare il consenso deve essere facile quanto esprimere: in tal modo l'interessato mantiene sempre un controllo effettivo sull'uso dei propri dati personali ⁽²⁴⁾.
- (20) In ultimo luogo, la legge sull'accesso ai dati e sul loro utilizzo chiarisce che, per valutare se il consenso è «manifestato liberamente», è necessario considerare se la prestazione di un servizio sia stata subordinata all'accettazione, da parte dell'interessato, del trattamento di dati personali anche se ciò non è richiesto per la prestazione di tale servizio. In caso affermativo la validità del consenso potrebbe essere compromessa ⁽²⁵⁾.

⁽¹⁸⁾ Considerando 67 della direttiva (UE) 2016/680.

⁽¹⁹⁾ Sentenza della Corte di giustizia Schrems («Schrems I»), C-362/14, ECLI:EU:C:2015:650, punto 73.

⁽²⁰⁾ Sentenza della Corte di giustizia Schrems («Schrems I»), C-362/14, ECLI:EU:C:2015:650, punto 74.

⁽²¹⁾ Cfr. comunicazione della Commissione al Parlamento europeo e al Consiglio, Scambio e protezione dei dati personali in un mondo globalizzato, COM(2017) 7 del 10.1.2017, sezione 3.1, pag. 7, disponibile al seguente indirizzo: <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52017DC0007>.

⁽²²⁾ Sezioni 33 e 40 A della legge del 2018 sulla protezione dei dati, introdotte dalla sezione 69, paragrafi 1, 2 e 4, della legge sull'accesso ai dati e sul loro utilizzo.

⁽²³⁾ Sezione 40 A, paragrafi 2 e 3, della legge del 2018 sulla protezione dei dati, introdotta dalla sezione 69, paragrafo 4, della legge sull'accesso ai dati e sul loro utilizzo.

⁽²⁴⁾ Sezione 40 A, paragrafi 5 e 6, della legge del 2018 sulla protezione dei dati, introdotta dalla sezione 69, paragrafo 4, della legge sull'accesso ai dati e sul loro utilizzo.

⁽²⁵⁾ Sezione 40 A, paragrafo 7, della legge del 2018 sulla protezione dei dati, introdotta dalla sezione 69, paragrafo 4, della legge sull'accesso ai dati e sul loro utilizzo.

- (21) È importante sottolineare che, in virtù della parte 3 riveduta della legge del 2018 sulla protezione dei dati, il consenso continua a non essere una base giuridica pertinente per le operazioni di trattamento che rientrano nell'ambito di applicazione della presente decisione, come spiegato al considerando 35 della decisione di esecuzione (UE) 2021/1773. Come rilevato al considerando 36 della decisione di esecuzione (UE) 2021/1773, in un contesto di contrasto, il trattamento continua a non essere possibile esclusivamente in base al consenso, dato che l'autorità competente deve disporre sempre di un potere di base che le consente di trattare i dati. Nello specifico, e analogamente a quanto autorizzato a norma della direttiva (UE) 2016/680⁽²⁶⁾, ciò significa che il consenso è una condizione aggiuntiva per permettere alcuni trattamenti limitati e specifici che non potrebbero essere svolti altrimenti, ad esempio la raccolta e il trattamento di un campione di DNA di una persona fisica che non è un indiziato.

2.2. **Garanzie, diritti e obblighi**

2.2.1. *Trattamento di dati personali sensibili*

- (22) Il quadro in materia di protezione dei dati del Regno Unito continua a fornire garanzie specifiche nel caso di categorie particolari di dati, come valutato nei considerando da 38 a 42 della decisione di esecuzione (UE) 2021/1773.
- (23) Sia la definizione di categorie particolari di dati personali sia le norme specifiche applicabili al trattamento di tali categorie di dati di cui alla legge del 2018 sulla protezione dei dati restano in vigore. Nel contempo la legge sull'accesso ai dati e sul loro utilizzo conferisce nuovi poteri normativi al segretario di Stato, il quale, se necessario, può aggiungere nuove categorie particolari di dati e adattare le condizioni applicabili al loro utilizzo⁽²⁷⁾. È importante sottolineare che tale potere non consente al segretario di Stato di sopprimere o modificare le categorie particolari di dati esistenti, né di modificarne le condizioni di trattamento⁽²⁸⁾.
- (24) Tali modifiche pertanto non incidono sul livello di protezione delle categorie particolari di dati personali ritenuto, nella decisione di esecuzione (UE) 2021/1773, sostanzialmente equivalente alla protezione all'interno dell'UE.

2.2.2. *Diritti delle persone fisiche*

- (25) Nel quadro giuridico del Regno Unito, gli interessati continuano a beneficiare degli stessi diritti individuali azionabili nei confronti del titolare del trattamento o del responsabile del trattamento di cui alla direttiva (UE) 2016/680, in particolare il diritto di accesso ai dati, il diritto di opporsi al trattamento e il diritto di far rettificare e cancellare i dati, di cui ai considerando da 57 a 65 della decisione di esecuzione (UE) 2021/1773.
- (26) La legge sull'accesso ai dati e sul loro utilizzo chiarisce alcune modalità di esercizio di tali diritti.
- (27) In primo luogo, in base al regime attuale, i titolari del trattamento hanno il diritto di rifiutarsi di dare seguito a una richiesta manifestamente infondata o eccessiva o di richiedere il pagamento di diritti ragionevoli⁽²⁹⁾. A tale riguardo, la legge sull'accesso ai dati e sul loro utilizzo conferisce al segretario di Stato un nuovo potere normativo che gli consente di emanare norme che impongono ai titolari del trattamento di produrre e pubblicare orientamenti in merito ai diritti addebitati in siffatte circostanze. Inoltre, quando respingono una richiesta per il summenzionato motivo, la legge sull'accesso ai dati e sul loro utilizzo ha chiarito che i titolari del trattamento continuano a essere tenuti a notificare all'interessato i motivi del rifiuto e il suo diritto di proporre reclamo all'ICO. Tale notifica deve essere fornita senza indebito ritardo⁽³⁰⁾.
- (28) In secondo luogo, la legge sull'accesso ai dati e sul loro utilizzo specifica i termini entro i quali i titolari del trattamento devono rispondere alle richieste dell'interessato. Più specificamente, allinea i termini di risposta a quelli del GDPR del Regno Unito. Le disposizioni rivedute consentono inoltre una proroga del termine di risposta che può

⁽²⁶⁾ Cfr. considerando 35 e 37 della direttiva (UE) 2016/680.

⁽²⁷⁾ Sezione 74 della legge sull'accesso ai dati e sul loro utilizzo. Tali regolamenti sono soggetti all'approvazione espressa (*affirmative resolution procedure*) del parlamento del Regno Unito.

⁽²⁸⁾ Cfr. la nuova sezione 42 A della legge del 2018 sulla protezione dei dati, introdotta dalla sezione 74 della legge sull'accesso ai dati e sul loro utilizzo, come pure le note esplicative della proposta di legge sull'accesso ai dati e sul loro utilizzo, paragrafo 577, disponibili al seguente indirizzo: <https://publications.parliament.uk/pa/bills/cbill/59-01/0179/en/240179en.pdf>.

⁽²⁹⁾ Sezione 53, paragrafo 1, della legge del 2018 sulla protezione dei dati. Cfr. anche considerando 64 della decisione di esecuzione (UE) 2021/1773.

⁽³⁰⁾ Sezione 53, paragrafi 4 A, 6 e 7, della legge del 2018 sulla protezione dei dati, introdotta dalla sezione 75 della legge sull'accesso ai dati e sul loro utilizzo.

giungere fino a due mesi supplementari qualora la richiesta sia complessa o quando trattasi di più richieste. In tali casi, il titolare del trattamento deve informare l'interessato della proroga e dei relativi motivi⁽³¹⁾. La legge sull'accesso ai dati e sul loro utilizzo ha inoltre introdotto un meccanismo che consente ai titolari del trattamento di sospendere il termine di risposta qualora l'interessato debba fornire ulteriori informazioni per identificare i dati richiesti⁽³²⁾.

- (29) In terzo luogo, per quanto riguarda solo il diritto di accesso alle informazioni e ai dati personali, la legge sull'accesso ai dati e sul loro utilizzo modifica la sezione 45 della legge del 2018 sulla protezione dei dati per integrare il chiarimento elaborato nell'ambito della giurisprudenza nazionale esistente sulla base del principio di proporzionalità ai sensi del diritto dell'UE, secondo cui i titolari del trattamento sono tenuti soltanto ad effettuare ricerche ragionevoli e proporzionate riguardo alle informazioni e ai dati personali richiesti⁽³³⁾. La nuova disposizione dovrebbe essere interpretata in linea con la giurisprudenza esistente, secondo la quale «[...] ciò che viene ponderato nell'esercizio di proporzionalità è l'oggetto finale della ricerca, vale a dire il potenziale vantaggio che la fornitura delle informazioni potrebbe apportare all'interessato, rispetto ai mezzi con cui tali informazioni sono ottenute. Occorre valutare in ogni singolo caso se saranno necessari sforzi sproporzionati per reperire e fornire le informazioni rispetto ai benefici che questo potrebbe apportare all'interessato»⁽³⁴⁾.
- (30) Pertanto, sebbene le modalità di risposta alle richieste degli interessati siano soggette a norme più dettagliate, il sistema del Regno Unito continua a garantire che tali richieste siano trattate entro termini ragionevoli definiti sulla base di fattori oggettivi. Inoltre, gli obblighi sostanziali di risposta alle richieste di accesso incombenti al titolare del trattamento sono definiti sulla base di norme giuridiche consolidate che tengono conto anche degli interessi dell'interessato. Infine, gli attuali orientamenti dell'ICO già prevedono che un titolare del trattamento non è tenuto a effettuare ricerche che sarebbero irragionevoli o sproporzionate rispetto all'importanza di fornire l'accesso alle informazioni⁽³⁵⁾.
- (31) Inoltre la legge sull'accesso ai dati e sul loro utilizzo ha introdotto una nuova sezione 45 A nella legge del 2018 sulla protezione dei dati, che prevede un'esenzione esplicita dall'obbligo di fornire accesso o informazioni a un interessato qualora tali informazioni siano protette dal segreto professionale⁽³⁶⁾. Questa esenzione si applica specificamente agli obblighi di cui alla sezione 44, paragrafo 2, e alla sezione 45, paragrafo 1, della legge del 2018 sulla protezione dei dati, che impongono ai titolari del trattamento di informare le persone fisiche in merito al trattamento dei loro dati personali e di concedere loro l'accesso a tali dati⁽³⁷⁾. Chiarisce che i titolari del trattamento non sono tenuti a divulgare informazioni qualora ciò violi il segreto professionale. Un'esenzione analoga è prevista dal GDPR del Regno Unito⁽³⁸⁾.
- (32) In termini di garanzie, i titolari del trattamento che si avvalgono di tale esenzione devono informare per iscritto e senza indebito ritardo l'interessato dell'applicazione della stessa, spiegarne i motivi e informarli del loro diritto di presentare ricorso all'Information Commission, o di esperire mezzi di ricorso⁽³⁹⁾. Per garantire la responsabilizzazione, la sezione 45 A, paragrafo 4, della legge del 2018 sulla protezione dei dati impone ai titolari del trattamento di conservare una traccia della motivazione della loro decisione di applicare l'esenzione e di metterla a disposizione dell'Information Commission su richiesta⁽⁴⁰⁾.

⁽³¹⁾ Sezione 54, paragrafi 3 A e b3, della legge del 2018 sulla protezione dei dati, introdotta dalla sezione 76, paragrafo 6, della legge sull'accesso ai dati e sul loro utilizzo.

⁽³²⁾ Sezione 54, paragrafi 3C e 3D, della legge del 2018 sulla protezione dei dati, introdotta dalla sezione 76, paragrafi 5 e 6, della legge sull'accesso ai dati e sul loro utilizzo.

⁽³³⁾ Sezione 45, paragrafo 2 A, della legge del 2018 sulla protezione dei dati, introdotta dalla sezione 78 della legge sull'accesso ai dati e sul loro utilizzo.

⁽³⁴⁾ *Dawson-Damer v Taylor Wessing LLP [2017] EWCA Civ 74.*

⁽³⁵⁾ Disponibili al seguente indirizzo: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/how-do-we-find-and-retrieve-the-relevant-information/>.

⁽³⁶⁾ Sezione 45 A, introdotta dalla sezione 79 della legge sull'accesso ai dati e sul loro utilizzo. Nel Regno Unito il segreto professionale è un diritto giuridico fondamentale che impedisce la divulgazione di specifiche comunicazioni riservate tra un cliente e il suo consulente legale senza il consenso del cliente stesso. Comprende due categorie principali: il segreto professionale riguardante la consulenza legale, che tutela gli scambi effettuati allo scopo di ottenere o fornire consulenza legale, e il segreto professionale riguardante il contenzioso, che si applica alle comunicazioni effettuate in preparazione o nel corso di procedimenti giudiziari.

⁽³⁷⁾ Le autorità competenti di cui alla parte 3 si sono precedentemente avvalse di altre esenzioni disponibili di cui alla sezione 44, paragrafo 4 (diritto di essere informati) e alla sezione 45, paragrafo 4 (diritto di accesso) della legge del 2018 sulla protezione dei dati.

⁽³⁸⁾ Allegato 2, paragrafo 19, della legge del 2018 sulla protezione dei dati.

⁽³⁹⁾ Sezione 45 A, paragrafo 2, della legge del 2018 sulla protezione dei dati, introdotta dalla sezione 79 della legge sull'accesso ai dati e sul loro utilizzo. Un'eccezione all'obbligo di notifica è prevista nel caso in cui la comunicazione stessa pregiudicherebbe la natura segreta o riservata delle informazioni. In tali casi, il titolare del trattamento non è tenuto a rivelare l'applicazione dell'esenzione né a fornire ulteriori spiegazioni.

⁽⁴⁰⁾ Sezione 45 A della legge del 2018 sulla protezione dei dati, introdotta dalla sezione 79 della legge sull'accesso ai dati e sul loro utilizzo.

- (33) Infine, la legge sull'accesso ai dati e sul loro utilizzo ha modificato e consolidato le esenzioni previste nella parte 3 della legge del 2018 sulla protezione dei dati, messe a disposizione delle autorità competenti a fini di sicurezza nazionale. L'esenzione per motivi di sicurezza nazionale consente alle autorità competenti di disapplicare talune disposizioni della parte 3 della legge del 2018 sulla protezione dei dati se l'esenzione da tale disposizione è necessaria al fine di salvaguardare la sicurezza nazionale⁽⁴¹⁾. L'esenzione rispecchia le esenzioni per motivi di sicurezza nazionale previste per il trattamento dei dati personali ai sensi del GDPR del Regno Unito (di cui alla sezione 26 della legge del 2018 sulla protezione dei dati) e della parte 4 della legge del 2018 sulla protezione dei dati (di cui alla sezione 110 della legge del 2018).
- (34) L'esenzione per motivi di sicurezza nazionale è soggetta alle stesse limitazioni e garanzie previste per le esenzioni ai sensi del GDPR del Regno Unito e della parte 4 della legge del 2018 sulla protezione dei dati, analizzate nei considerando da 64 a 67 e 126 della decisione di esecuzione (UE) 2021/1772. In particolare, l'esenzione può essere applicata soltanto se necessaria per salvaguardare la sicurezza nazionale. Non si tratta di un'esenzione generalizzata e deve essere presa in considerazione e invocata dal titolare del trattamento caso per caso⁽⁴²⁾. Inoltre qualsiasi applicazione dell'esenzione deve essere conforme alle norme in materia di diritti umani (sostenute dalla legge del 1998 sui diritti umani e dalla convenzione europea dei diritti dell'uomo), secondo le quali qualsiasi ingerenza rispetto ai diritti in materia di tutela della vita privata dovrebbe essere necessaria e proporzionata in una società democratica⁽⁴³⁾. Ciò è confermato anche dagli orientamenti dell'ICO sull'applicazione delle esenzioni per motivi di sicurezza nazionale⁽⁴⁴⁾.

2.2.3. Limitazioni ai trasferimenti successivi

- (35) Il livello di protezione offerto ai dati personali trasferiti dall'Unione europea alle autorità di contrasto nel Regno Unito continua a non essere compromesso da ulteriori trasferimenti di tali dati a destinatari che si trovano in un paese terzo. Il regime in materia di trasferimenti internazionali di dati personali dal Regno Unito rimane molto simile alle norme di cui al capo V della direttiva (UE) 2016/680, come valutato nei considerando da 74 a 87 della decisione di esecuzione (UE) 2021/1773.
- (36) Sebbene la legge sull'accesso ai dati e sul loro utilizzo abbia modificato la parte 3, capo 5, della legge del 2018 sulla protezione dei dati relativo ai trasferimenti di dati personali alle autorità competenti di paesi terzi, essa mantiene la disposizione centrale secondo cui a) il trasferimento deve essere necessario per una finalità di contrasto, b) il trasferimento i) deve essere basato su regolamenti che approvano il trasferimento (che sostituiscono i precedenti regolamenti di adeguatezza), ii) è soggetto a garanzie adeguate, o iii) si basa su circostanze speciali, e c) il destinatario del trasferimento deve essere: i) un'autorità competente (ossia l'equivalente di un'autorità competente) nel paese terzo; ii) un'organizzazione internazionale pertinente, iii) un responsabile del trattamento che tratta i dati per conto di un'autorità competente, o iv) una persona diversa da un'autorità competente, ma solo se il trasferimento è strettamente necessario per lo svolgimento di una delle finalità di contrasto⁽⁴⁵⁾. Tali principi generali alla base dei trasferimenti di dati sono ripresi nella sezione 73 della legge del 2018 sulla protezione dei dati, secondo la quale, tra l'altro, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale sono consentiti solo se il trasferimento è effettuato in conformità delle altre disposizioni della parte 3 della legge del 2018 sulla protezione dei dati⁽⁴⁶⁾.
- (37) Per quanto riguarda specificamente i regolamenti che approvano un trasferimento, la sezione 74AA, paragrafo 2, della legge del 2018 sulla protezione dei dati precisa che il segretario di Stato può adottare tali regolamenti solo se ritiene che la verifica della protezione dei dati sia soddisfatta. Ciò significa che la possibilità per il segretario di Stato, introdotta nella sezione 74AA, paragrafo 3, della legge del 2018 sulla protezione dei dati, di tenere conto dell'opportunità di agevolare i flussi di dati nell'elaborazione di tali regolamenti è sempre subordinata al soddisfacimento della verifica della protezione dei dati. La nuova sezione 74AB⁽⁴⁷⁾ della legge del 2018 sulla protezione dei dati enuncia il criterio giuridico per il soddisfacimento della verifica della protezione dei dati, imponendo che il livello di protezione degli interessati nei paesi o nelle organizzazioni internazionali destinatari non sia sostanzialmente inferiore a quello previsto dalla pertinente legislazione del Regno Unito in materia di protezione

⁽⁴¹⁾ Sezione 78 A, paragrafo 1, della legge del 2018 sulla protezione dei dati, introdotta dalla sezione 88 della legge sull'accesso ai dati e sul loro utilizzo. Ai sensi della sezione 78 A, paragrafi da 2 a 4, della legge del 2018 sulla protezione dei dati, l'esenzione consente di disapplicare i principi in materia di protezione dei dati (fatta eccezione per il principio di liceità e le condizioni e garanzie per il trattamento dei dati sensibili), i diritti individuali, gli obblighi dei titolari del trattamento e dei responsabili del trattamento in relazione alle violazioni dei dati, alcune parti delle norme sui trasferimenti internazionali di dati e alcuni dei poteri di accesso dell'Information Commissioner per lo svolgimento di ispezioni e l'adozione di azioni esecutive.

⁽⁴²⁾ Cfr. *Baker v Secretary of State for the Home Department* [2001] UKIT NSA2 («*Baker v Secretary of State*»).

⁽⁴³⁾ Cfr. anche *Guriev v Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), punto 45; *Lin v Commissioner of the Police for the Metropolis* [2015] EWHC 2484 (QB), punto 80.

⁽⁴⁴⁾ Cfr. gli orientamenti dell'ICO sull'eccezione per motivi di sicurezza nazionale e difesa, disponibili al seguente indirizzo: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/>.

⁽⁴⁵⁾ Sezione 73 della legge del 2018 sulla protezione dei dati, come modificata dal paragrafo 3, punti 4 e 5, dell'allegato 8 della legge sull'accesso ai dati e sul loro utilizzo.

⁽⁴⁶⁾ Sezione 73 della legge del 2018 sulla protezione dei dati, come modificata dal paragrafo 3, punto 3, dell'allegato 8 della legge sull'accesso ai dati e sul loro utilizzo.

⁽⁴⁷⁾ Introdotta dal paragrafo 4, punto 2, dell'allegato 8 della legge sull'accesso ai dati e sul loro utilizzo.

dei dati. La sezione 74AB, paragrafo 2, della legge del 2018 sulla protezione dei dati fornisce un elenco non esaustivo di elementi da considerare nel valutare se tale verifica è soddisfatta, quali il rispetto dello Stato di diritto e dei diritti umani, la presenza di un'autorità di protezione dei dati e le sue competenze, le modalità di ricorso giurisdizionale o extragiudiziale, le norme sul trasferimento di dati personali dal paese o dall'organizzazione ad altri paesi o organizzazioni internazionali, i pertinenti obblighi internazionali del paese o dell'organizzazione e la costituzione, le tradizioni e la cultura del paese o dell'organizzazione. Nel riformulare l'elenco degli elementi pertinenti di cui alla previgente sezione 74 A della legge del 2018 sulla protezione dei dati, la nuova disposizione mantiene gli elementi centrali di tale elenco e rimane pertanto simile alle disposizioni dell'articolo 36 della direttiva (UE) 2016/680. Le autorità del Regno Unito hanno inoltre confermato che il segretario di Stato terrà conto di elementi non previsti alla sezione 74AB, paragrafo 2, quali le leggi e le prassi di un paese terzo relative al modo in cui le autorità pubbliche accedono ai dati personali per finalità quali la sicurezza nazionale o l'applicazione della legge, nella misura in cui queste incidono sul livello generale di protezione. Inoltre le autorità del Regno Unito ritengono che la giurisprudenza pertinente del paese terzo sarà una componente essenziale in sede di considerazione delle questioni elencate in modo non esaustivo alla sezione 74AB, paragrafo 2, della legge del 2018 sulla protezione dei dati.

- (38) I regolamenti che approvano un trasferimento continuano a essere soggetti ai requisiti procedurali «generali» previsti dalla sezione 182 della legge del 2018 sulla protezione dei dati, come indicato al considerando 77 della decisione di esecuzione (UE) 2021/1773. Secondo tale procedura, quando propone futuri regolamenti di adeguatezza del Regno Unito il segretario di Stato deve consultare l'Information Commissioner⁽⁴⁸⁾. Una volta adottati dal segretario di Stato, tali regolamenti sono presentati al parlamento e sottoposti alla procedura di «risoluzione negativa» nel contesto della quale entrambe le camere del parlamento possono esaminare i regolamenti e hanno la facoltà di presentare una mozione di annullamento dei regolamenti stessi entro un termine di 40 giorni⁽⁴⁹⁾.
- (39) Per quanto riguarda le garanzie adeguate, la sezione 75 della legge del 2018 sulla protezione dei dati, come modificata dall'allegato 8, paragrafo 6, della legge sull'accesso ai dati e sul loro utilizzo, stabilisce che tali trasferimenti possono essere effettuati solo se: a) il destinatario previsto dei dati è vincolato da uno strumento giuridico adeguato, vale a dire uno strumento che soddisfa le condizioni di cui al nuovo paragrafo 4, in particolare la condizione secondo cui ciascuna autorità competente del Regno Unito che fa parte dello strumento, agendo in modo ragionevole e proporzionato, ritiene che la verifica della protezione dei dati sia soddisfatta, o b) il titolare del trattamento, agendo in modo ragionevole e proporzionato, ritiene che la verifica della protezione dei dati sia soddisfatta in relazione al trasferimento o al tipo di trasferimento. La sezione 75, paragrafo 5, inserita nella legge del 2018 sulla protezione dei dati chiarisce che la verifica della protezione dei dati è soddisfatta se dopo il trasferimento, grazie alle garanzie imposte, il livello di protezione previsto per gli interessati non è sostanzialmente inferiore al livello previsto dalla pertinente legislazione del Regno Unito in materia di protezione dei dati. Tali misure sono simili a quelle previste all'articolo 37 della direttiva (UE) 2016/680. Pertanto nell'UE e nel Regno Unito si applicano gli stessi criteri giuridici per quanto riguarda l'approvazione di un trasferimento soggetto a garanzie adeguate. A norma della nuova sezione 75, paragrafo 6, della legge del 2018 sulla protezione dei dati, ciò che è ragionevole e proporzionato deve essere determinato con riferimento a tutte le circostanze, o alle circostanze probabili, del trasferimento o del tipo di trasferimento, compresi la natura e il volume dei dati personali trasferiti.
- (40) Per quanto riguarda i trasferimenti basati su circostanze particolari a norma della sezione 76 della legge del 2018 sulla protezione dei dati, sono introdotte diverse modifiche tecniche che chiariscono le condizioni in base alle quali tali trasferimenti possono avvenire, ma che non incidono sul livello di protezione dei dati personali nel Regno Unito⁽⁵⁰⁾.
- (41) In termini di attuazione delle norme del Regno Unito in materia di trasferimenti internazionali, dall'adozione della decisione di esecuzione (UE) 2021/1773 sono intervenuti diversi sviluppi.
- (42) In primo luogo, a seguito della conclusione, nel 2022, di un memorandum d'intesa tra il ministero degli Interni e l'ICO, che ha definito i rispettivi ruoli nello svolgimento delle valutazioni dell'adeguatezza delle attività di contrasto⁽⁵¹⁾, il Regno Unito ha effettuato valutazioni dei quadri in materia di protezione dei dati nei Balati di Jersey

⁽⁴⁸⁾ Cfr. il protocollo d'intesa tra il segretario di Stato del dipartimento per il Digitale, la cultura, i media e lo sport e l'ICO sul ruolo dell'ICO in relazione alla nuova valutazione dell'adeguatezza del Regno Unito, disponibile al seguente indirizzo: <https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments>.

⁽⁴⁹⁾ Laddove tale votazione abbia esito positivo, i regolamenti cesseranno in definitiva di avere ulteriore effetto giuridico.

⁽⁵⁰⁾ Allegato 8, paragrafo 7, della legge sull'accesso ai dati e sul loro utilizzo.

⁽⁵¹⁾ Disponibile al seguente indirizzo: <https://ico.org.uk/media2/about-the-ico/mou/4025752/ico-ho-mou.pdf>.

e Guernsey e nell'Isola di Man. Di conseguenza il Regno Unito ha adottato i regolamenti di adeguatezza per Guernsey⁽⁵²⁾ nel luglio 2023, per Jersey⁽⁵³⁾ nel novembre 2023 e per l'Isola di Man⁽⁵⁴⁾ nel gennaio 2025. Tali regolamenti confermano che ciascuna giurisdizione garantisce un livello di protezione adeguato dei dati personali trasferiti a norma della parte 3 della legge del 2018 sulla protezione dei dati. Sebbene tali regolamenti siano stati originariamente adottati nell'ambito del precedente quadro giuridico, la valutazione su cui si fondano rimane valida nell'ambito del quadro aggiornato. Pertanto i regolamenti continuano a facilitare la cooperazione internazionale nell'ambito delle attività di contrasto.

- (43) Nel valutare il funzionamento delle decisioni di adeguatezza adottate sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46/CE conformemente all'articolo 97 del regolamento (UE) 2016/679, la Commissione ha inoltre esaminato i quadri in materia di protezione dei dati per il trattamento dei dati personali nell'ambito delle attività di contrasto in materia penale, nonché le norme sull'accesso ai dati personali da parte delle autorità pubbliche per motivi di sicurezza nazionale nei Balati di Jersey e Guernsey e nell'Isola di Man. Sulla base, tra l'altro, di tale valutazione, la Commissione ha concluso che tutte e tre le giurisdizioni continuano a offrire un livello adeguato di protezione dei dati personali trasferiti dall'UE⁽⁵⁵⁾.
- (44) In secondo luogo, nel 2022 il Regno Unito e gli Stati Uniti hanno concluso un accordo sulla protezione dei dati e la vita privata⁽⁵⁶⁾, che applica mutatis mutandis i termini dell'accordo quadro UE-USA⁽⁵⁷⁾, garantendo protezioni equivalenti nel contesto degli scambi di dati tra il Regno Unito e gli Stati Uniti a fini di contrasto.
- (45) In terzo luogo, nel 2023 e nel 2025 l'ICO ha aggiornato i propri orientamenti sui trasferimenti internazionali di cui alla parte 3, capo 5, della legge del 2018 sulla protezione dei dati⁽⁵⁸⁾. L'aggiornamento del 2023 ha chiarito il significato del requisito «strettamente necessario» per i trasferimenti di dati a destinatari diversi dalle competenti autorità di contrasto, offrendo così maggiore certezza ai titolari del trattamento che valutano la legittimità di tali trasferimenti. Nel 2025 l'elenco dei paesi e territori adeguati è stato aggiornato a seguito dei regolamenti di adeguatezza del Regno Unito per l'Isola di Man.

2.2.4. *Processo decisionale automatizzato*

- (46) Pur mantenendo diversi elementi delle norme sul processo decisionale automatizzato valutati nei considerando 72 e 73 della decisione di esecuzione (UE) 2021/1773, la legge sull'accesso ai dati e sul loro utilizzo ne ha modificato alcuni aspetti.
- (47) In primo luogo, la nuova sezione 50B della legge del 2018 sulla protezione dei dati stabilisce un divieto generale nei confronti di decisioni significative basate, interamente o parzialmente, sul trattamento di categorie particolari di dati personali. Sono tuttavia previste due eccezioni a tale divieto: l'interessato ha manifestato il proprio consenso esplicito a tale trattamento, oppure la decisione è imposta o autorizzata per legge⁽⁵⁹⁾.
- (48) In secondo luogo, la nuova sezione 50C della legge del 2018 sulla protezione dei dati impone ai titolari del trattamento di attuare garanzie per qualsiasi decisione significativa basata, interamente o parzialmente, su dati personali e basata unicamente su un trattamento automatizzato. Tali garanzie devono includere l'informazione

⁽⁵²⁾ Disponibili al seguente indirizzo: <https://www.legislation.gov.uk/uksi/2023/1221/contents/made>.

⁽⁵³⁾ Disponibili al seguente indirizzo: <https://www.legislation.gov.uk/uksi/2023/744/made>.

⁽⁵⁴⁾ Disponibili al seguente indirizzo: <https://www.legislation.gov.uk/uksi/2025/89/contents/made>.

⁽⁵⁵⁾ Relazione della Commissione al Parlamento europeo e al Consiglio sul primo riesame del funzionamento delle decisioni di adeguatezza adottate a norma dell'articolo 25, paragrafo 6, della direttiva 95/46/CE, del 15 gennaio 2024, disponibile al seguente indirizzo: <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52024DC0007>; e relazioni per paese sul funzionamento delle decisioni di adeguatezza adottate a norma della direttiva 95/46/CE che accompagnano la relazione della Commissione al Parlamento europeo e al Consiglio sul primo riesame del funzionamento delle decisioni di adeguatezza adottate a norma dell'articolo 25, paragrafo 6, della direttiva 95/46/CE, disponibili al seguente indirizzo:

https://commission.europa.eu/document/download/f8229eb2-1a36-4cf5-a099-1cd001664bff_en?filename=JUST_template_coming_soon_Commission%20Staff%20Working%20Document%20-%20Report%20on%20the%20first%20review%20of%20the%20functioning.pdf.

⁽⁵⁶⁾ Disponibile al seguente indirizzo: <https://www.gov.uk/government/publications/ukusa-exchange-of-notes-on-the-protection-of-personal-information-relating-to-prevention-investigation-detection-and-prosecution-of-criminal-offence>.

⁽⁵⁷⁾ 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, pag. 3), disponibile al seguente indirizzo: [https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:22016A1210\(01\)&from=EN](https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN).

⁽⁵⁸⁾ Disponibili al seguente indirizzo: <https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/international-transfers/>.

⁽⁵⁹⁾ Sezione 50B della legge del 2018 sulla protezione dei dati, introdotta dalla sezione 80, paragrafo 3, della legge sull'accesso ai dati e sul loro utilizzo.

dell'interessato in merito al processo decisionale, consentendogli di contestare la decisione o presentare osservazioni e di richiedere l'intervento umano nel processo decisionale⁽⁶⁰⁾. Sebbene la sezione 50C, paragrafo 4, della legge del 2018 sulla protezione dei dati introduca un'esenzione dall'applicazione di tali garanzie laddove questa sia necessaria per non ostacolare indagini, inchieste o procedimenti ufficiali o giudiziari, per non compromettere la prevenzione, l'accertamento, l'indagine o il perseguimento di reati o l'esecuzione di sanzioni penali, per tutelare la sicurezza pubblica, per salvaguardare la sicurezza nazionale o i diritti e le libertà altrui, l'applicazione di tali garanzie è sospesa solo temporaneamente, dato che il titolare del trattamento è tenuto a riesaminare la decisione non appena ragionevolmente possibile e tale riesame prevede un coinvolgimento umano significativo⁽⁶¹⁾.

- (49) Inoltre la nuova sezione 50 A della legge del 2018 sulla protezione dei dati chiarisce la definizione di decisione «basata unicamente su un trattamento automatizzato» stabilendo che si tratta di una decisione in cui non vi è alcun coinvolgimento umano significativo nel processo decisionale. È importante sottolineare che i titolari del trattamento, per determinare se il coinvolgimento umano è stato significativo, sono tenuti a valutare in che misura la profilazione contribuisca a una decisione. La sezione 50 A della legge del 2018 sulla protezione dei dati chiarisce inoltre che per «decisione significativa» si intende una decisione che produce effetti giuridici negativi o che, in modo analogo, incide significativamente su un interessato in modo negativo⁽⁶²⁾. Tale limitazione delle decisioni che hanno un effetto negativo sull'interessato riflette il fatto che, a differenza del trattamento ai sensi del GDPR del Regno Unito, è improbabile che le autorità competenti adottino decisioni ritenute positive dagli interessati.
- (50) Infine, la nuova sezione 50D della legge del 2018 sulla protezione dei dati conferisce al segretario di Stato il potere di adottare atti di diritto derivato per definire cosa costituisca un coinvolgimento umano significativo e quali decisioni debba essere considerate come aventi un effetto negativo altrettanto significativo sugli interessati. Questa sezione consente inoltre al segretario di Stato di adottare atti di diritto derivato per i) aggiungere nuove garanzie; ii) imporre prescrizioni che integrino le garanzie esistenti; iii) definire le misure che non soddisfano le garanzie⁽⁶³⁾. È importante sottolineare che, prima di adottare regolamenti conformemente alla sezione 50D della legge del 2018 sulla protezione dei dati, il segretario di Stato deve consultare l'ICO⁽⁶⁴⁾; inoltre i regolamenti sono soggetti all'approvazione espressa⁽⁶⁵⁾, il che significa che devono essere approvati da entrambe le camere del parlamento del Regno Unito prima di poter essere adottati.
- (51) Sebbene la legge sull'accesso ai dati e sul loro utilizzo abbia quindi modificato il quadro del processo decisionale automatizzato, è importante osservare che, nell'ambito del quadro giuridico del Regno Unito, il processo decisionale automatizzato continua ad essere soggetto alla garanzia fondamentale che protegge il diritto di ottenere l'intervento umano in tutti i casi di processo decisionale automatizzato, ossia sulla base del trattamento di dati personali sensibili e non sensibili⁽⁶⁶⁾.

2.2.5. Responsabilizzazione

- (52) Il quadro giuridico del Regno Unito continua a sostenere il principio di responsabilizzazione sancito dalla direttiva (UE) 2016/680, che impone alle autorità pubbliche di attuare misure tecniche e organizzative adeguate per assicurare e dimostrare il rispetto degli obblighi in materia di protezione dei dati, come valutato nei considerando da 88 a 92 della decisione di esecuzione (UE) 2021/1773.
- (53) Una delle misure comprese nella legge del 2018 sulla protezione dei dati, volte a garantire la responsabilizzazione e consentire ai titolari del trattamento e ai responsabili del trattamento di dimostrare la conformità, è l'obbligo per le autorità competenti di mantenere registri di tutte le attività legate al trattamento, comprese la raccolta, la modifica, la consultazione, la divulgazione, l'interconnessione e la cancellazione di dati personali⁽⁶⁷⁾. La legge sull'accesso ai dati e sul loro utilizzo modifica gli obblighi specifici dei titolari del trattamento, di cui a tale disposizione, semplicemente eliminando nella sezione 62 della legge del 2018 sulla protezione dei dati l'obbligo dei titolari del trattamento di registrare una giustificazione quando i dati personali sono consultati o divulgati⁽⁶⁸⁾. È importante sottolineare che rimane in vigore l'obbligo dei titolari del trattamento di registrare le attività legate al trattamento in quanto tali, cosicché il principale meccanismo di garanzia della responsabilizzazione è preservato.

⁽⁶⁰⁾ Sezione 50C della legge del 2018 sulla protezione dei dati, introdotta dalla sezione 80, paragrafo 3, della legge sull'accesso ai dati e sul loro utilizzo.

⁽⁶¹⁾ Sezione 50C, paragrafi 3 e 4, della legge del 2018 sulla protezione dei dati, introdotta dalla sezione 80, paragrafo 3, della legge sull'accesso ai dati e sul loro utilizzo.

⁽⁶²⁾ Sezione 50 A della legge del 2018 sulla protezione dei dati, introdotta dalla sezione 80, paragrafo 3, della legge sull'accesso ai dati e sul loro utilizzo.

⁽⁶³⁾ Sezione 50D della legge del 2018 sulla protezione dei dati, introdotta dalla sezione 80, paragrafo 3, della legge sull'accesso ai dati e sul loro utilizzo. Qualsiasi norma adottata nell'ambito di tali poteri è soggetta all'approvazione espressa (*affirmative resolution procedure*), che garantisce il controllo parlamentare. I regolamenti non possono modificare le disposizioni della sezione 50C.

⁽⁶⁴⁾ Sezione 182, paragrafo 2, della legge del 2018 sulla protezione dei dati.

⁽⁶⁵⁾ Sezione 50D, paragrafo 5, della legge del 2018 sulla protezione dei dati.

⁽⁶⁶⁾ Sezione 50C, paragrafo 2, lettera c), della legge del 2018 sulla protezione dei dati.

⁽⁶⁷⁾ Sezione 62 della legge del 2018 sulla protezione dei dati. Cfr. anche considerando 90 della decisione di esecuzione (UE) 2021/1773.

⁽⁶⁸⁾ Sezione 82 della legge sull'accesso ai dati e sul loro utilizzo.

2.3. Vigilanza e applicazione

2.3.1. Vigilanza indipendente

- (54) Nel Regno Unito continua a spettare a un'autorità indipendente di controllo della protezione dei dati il compito di controllare e fare applicare il quadro in materia di protezione dei dati, come analizzato nei considerando da 93 a 99 della decisione di esecuzione (UE) 2021/1773. La legge sull'accesso ai dati e sul loro utilizzo riforma la struttura di governance di tale autorità istituendo un'entità giuridica, l'Information Commission, che sostituirà l'ICO, strutturata come una «corporation sole».
- (55) Più specificamente, le misure di governance previste dalla legge sull'accesso ai dati e sul loro utilizzo, una volta attuate, aboliranno l'ufficio dell'Information Commissioner e trasferiranno le funzioni, il personale e i beni dall'ICO alla nuova entità, l'Information Commission. L'Information Commission è composta da membri con e senza incarichi esecutivi⁽⁶⁹⁾. La legge affida all'Information Commissioner, uno dei membri senza incarichi esecutivi, il ruolo di presidente dell'Information Commission⁽⁷⁰⁾. La legge sull'accesso ai dati e sul loro utilizzo prevede inoltre che, nella misura in cui ciò sia opportuno in conseguenza del trasferimento di funzioni, i riferimenti all'Information Commissioner in tutti gli atti normativi o in altri documenti (ogniqualvolta siano stati approvati o redatti) siano considerati come riferimenti all'Information Commission. Per l'esercizio delle sue funzioni, l'Information Commission può istituire comitati e delegare funzioni a un membro, a un dipendente o a un comitato dell'Information Commission⁽⁷¹⁾ e può adottare disposizioni per disciplinare la sua procedura e quella dei comitati, anche per quanto riguarda il quorum e l'adozione di decisioni a maggioranza. Tali procedure devono essere rese pubbliche⁽⁷²⁾.
- (56) È importante sottolineare che l'indipendenza dell'Information Commission è soggetta, anche per quanto riguarda le norme relative alla nomina e alla revoca del suo presidente, alle stesse garanzie che sono state citate nei considerando da 95 a 98 della decisione di esecuzione (UE) 2021/1773⁽⁷³⁾. Analoghe tutele si applicano agli altri membri senza incarichi esecutivi dell'Information Commission. In particolare, il presidente dell'Information Commission è nominato dal Re su raccomandazione del segretario di Stato. È selezionato sulla base del merito nell'ambito di un concorso equo e aperto⁽⁷⁴⁾. Gli altri membri senza incarichi esecutivi sono nominati dal segretario di Stato previa consultazione del presidente. I candidati possono essere raccomandati per la nomina o nominati solo se selezionati sulla base del merito nell'ambito di un concorso equo e aperto e se il segretario di Stato ha accertato che non si trovano in una situazione di conflitto di interessi⁽⁷⁵⁾. I membri con incarichi esecutivi sono assunti dall'Information Commission alle condizioni stabilite dai membri senza incarichi esecutivi⁽⁷⁶⁾. Il direttore esecutivo è nominato dal presidente e da altri membri senza incarichi esecutivi, previa consultazione del segretario di Stato. Anche le nomine dei membri con incarichi esecutivi sono soggette a una selezione sulla base del merito nell'ambito di un concorso equo e aperto⁽⁷⁷⁾.
- (57) Il presidente può essere revocato solo dal Re su indirizzo di entrambe le camere del parlamento e solo se il segretario di Stato ha presentato una relazione alla camera in questione in cui dichiara di aver accertato che il presidente si è reso colpevole di gravi negligenze, si trova in situazione di conflitto di interessi, non ha assolto obblighi specifici di informazione in merito a potenziali conflitti di interessi o non è in grado, non è idoneo o non è disposto a svolgere le funzioni di presidente⁽⁷⁸⁾. I membri senza incarichi esecutivi possono essere rimossi dall'incarico dal segretario di Stato solo se sono soddisfatte le condizioni specifiche stabilite dalla legislazione. Tra queste figurano una situazione di conflitto di interessi, gravi negligenze o incapacità, indisponibilità o inidoneità a svolgere le proprie funzioni. In termini di garanzie supplementari, il segretario di Stato è tenuto a rendere pubblica la decisione di procedere in tal senso e a fornire al membro in questione una dichiarazione attestante i motivi della rimozione dall'incarico⁽⁷⁹⁾.

⁽⁶⁹⁾ Paragrafo 3, punto 1, dell'allegato 12 A della legge del 2018 sulla protezione dei dati.

⁽⁷⁰⁾ Sezioni 117, 118, 119 e 120 in combinato disposto con l'allegato 14 della legge sull'accesso ai dati e sul loro utilizzo.

⁽⁷¹⁾ Paragrafi 13 e 14 dell'allegato 12 A della legge del 2018 sulla protezione dei dati.

⁽⁷²⁾ Paragrafo 16 dell'allegato 12 A della legge del 2018 sulla protezione dei dati.

⁽⁷³⁾ Articolo 52 del GDPR del Regno Unito e allegato 12 A della legge del 2018 sulla protezione dei dati, introdotto dalla sezione 117 della legge sull'accesso ai dati e sul loro utilizzo.

⁽⁷⁴⁾ Paragrafo 5, punto 1, dell'allegato 12 A della legge del 2018 sulla protezione dei dati.

⁽⁷⁵⁾ Paragrafo 3, punto 2, e paragrafi 5 e 6, dell'allegato 12 A della legge del 2018 sulla protezione dei dati.

⁽⁷⁶⁾ Paragrafo 11 dell'allegato 12 A della legge del 2018 sulla protezione dei dati.

⁽⁷⁷⁾ Paragrafo 5, punto 2, dell'allegato 12 A della legge del 2018 sulla protezione dei dati.

⁽⁷⁸⁾ Paragrafo 7, punti 6 e 7, dell'allegato 12 A della legge del 2018 sulla protezione dei dati.

⁽⁷⁹⁾ Paragrafo 9, punti 6, 7, 8 e 9, dell'allegato 12 A della legge del 2018 sulla protezione dei dati.

- (58) La legge sull'accesso ai dati e sul loro utilizzo non modifica le responsabilità centrali dell'Information Commission, che continuerà a svolgere le funzioni di cui all'allegato 13 della legge del 2018 sulla protezione dei dati. Tra queste figurano il monitoraggio e la responsabilità di imporre il rispetto della parte 3 della legge del 2018 sulla protezione dei dati, la consulenza al parlamento e al governo, la sensibilizzazione del pubblico, il sostegno ai responsabili del trattamento e ai titolari del trattamento nell'adempimento dei loro obblighi e l'informazione delle persone in merito ai loro diritti ⁽⁸⁰⁾. La legge sull'accesso ai dati e sul loro utilizzo chiarisce che, nell'esercizio del proprio dovere di garantire un livello adeguato di protezione dei dati personali, l'Information Commission dovrà tenere conto degli interessi degli interessati, dei titolari del trattamento e di altri soggetti e considerare l'interesse pubblico generale; dovrà inoltre promuovere tra il pubblico un clima di fiducia nel trattamento dei dati personali ⁽⁸¹⁾.
- (59) Inoltre la legge sull'accesso ai dati e sul loro utilizzo specifica che l'Information Commission, nello svolgimento delle sue funzioni a norma della legislazione in materia di protezione dei dati, deve prendere in considerazione, nella misura in cui siano pertinenti nelle circostanze del caso, la promozione dell'innovazione e della concorrenza, l'importanza della prevenzione, dell'indagine, dell'accertamento e del perseguimento dei reati, la necessità di salvaguardare la pubblica sicurezza e la sicurezza nazionale e le esigenze specifiche connesse alla protezione dei minori ⁽⁸²⁾. Il diritto dell'UE in materia di protezione dei dati riconosce inoltre la necessità di trovare un equilibrio tra la protezione dei dati personali e diversi altri diritti e obiettivi fondamentali, quali la sicurezza e la giustizia ⁽⁸³⁾.

2.3.2. *Applicazione, comprese le sanzioni, e mezzi di ricorso*

- (60) I poteri e i compiti dell'Information Commission continuano a corrispondere a quelli delle autorità di controllo della protezione dei dati degli Stati membri a norma dei pertinenti articoli della direttiva (UE) 2016/680 ⁽⁸⁴⁾, come valutato nei considerando da 100 a 109 della decisione di esecuzione (UE) 2021/1773.
- (61) La legge sull'accesso ai dati e sul loro utilizzo ha introdotto alcuni chiarimenti in merito all'esercizio di alcuni di tali poteri.
- (62) La sezione 97 della legge sull'accesso ai dati e sul loro utilizzo modifica la sezione 142 della legge del 2018 sulla protezione dei dati consentendo espressamente all'Information Commission di richiedere non solo informazioni ma anche documenti specifici, rafforzandone in tal modo la capacità di indagine e verifica dell'adempienza.
- (63) La sezione 98 della legge sull'accesso ai dati e sul loro utilizzo rafforza i poteri dell'Information Commission di cui alla sezione 146 della legge del 2018 sulla protezione dei dati, consentendole di chiedere a un titolare del trattamento o a un responsabile del trattamento di commissionare una relazione indipendente su una questione specifica. La relazione deve essere redatta da una «persona autorizzata» e l'Information Commission ha il potere di approvare in via definitiva il candidato o di nominarne uno se nessun candidato idoneo è proposto o se il titolare del trattamento omette di agire ⁽⁸⁵⁾. L'avviso di valutazione può specificare il formato, il contenuto e il termine di scadenza della relazione ⁽⁸⁶⁾. Tutti i costi inerenti, compresi gli onorari della persona autorizzata, devono essere sostenuti dal titolare del trattamento o dal responsabile del trattamento ⁽⁸⁷⁾.
- (64) La sezione 100 della legge sull'accesso ai dati e sul loro utilizzo istituisce un nuovo strumento di applicazione, gli avvisi formali di comparizione (*interview notices*), ai sensi della sezione 148 A della legge del 2018 sulla protezione dei dati. L'Information Commission può imporre a una persona di presentarsi, assicurando garanzie quali la protezione contro l'autoincriminazione e il segreto professionale ⁽⁸⁸⁾.
- (65) La sezione 101 della legge sull'accesso ai dati e sul loro utilizzo modifica l'allegato 16 della legge del 2018 sulla protezione dei dati riconoscendo all'Information Commission una maggiore flessibilità nell'emissione di avvisi di irrogazione di sanzioni. Sebbene l'attuale termine di sei mesi per l'emissione di un avviso definitivo di irrogazione di sanzioni successivo a una comunicazione di avvio del procedimento rimanga la regola generale, la sezione consente all'Information Commission di emettere tale avviso anche oltre il termine stabilito qualora non sia ragionevolmente possibile rispettarlo. In tali casi, l'avviso deve essere emesso non appena ragionevolmente possibile. Inoltre, qualora decida di non emettere detto avviso, l'Information Commission deve informare l'interessato per iscritto entro sei mesi o non appena ragionevolmente possibile. La sezione introduce inoltre un nuovo obbligo a carico dell'Information Commission, chiamata a pubblicare orientamenti sulle circostanze in cui potrebbero essere necessari più di sei mesi per emettere un avviso di irrogazione di sanzioni.

⁽⁸⁰⁾ Allegato 13 della legge del 2018 sulla protezione dei dati.

⁽⁸¹⁾ Sezione 91 della legge sull'accesso ai dati e sul loro utilizzo, che introduce la sezione 120 A della legge del 2018 sulla protezione dei dati.

⁽⁸²⁾ Sezione 91 della legge sull'accesso ai dati e sul loro utilizzo, che introduce la sezione 120B della legge del 2018 sulla protezione dei dati.

⁽⁸³⁾ Cfr. in particolare il considerando 2 della direttiva (UE) 2016/680.

⁽⁸⁴⁾ Paragrafo 2 dell'allegato 13 della legge del 2018 sulla protezione dei dati.

⁽⁸⁵⁾ Sezione 98 della legge sull'accesso ai dati e sul loro utilizzo, che introduce la sezione 146 A della legge del 2018 sulla protezione dei dati.

⁽⁸⁶⁾ Sezione 98 della legge sull'accesso ai dati e sul loro utilizzo che introduce la sezione 146, paragrafo 3 A, della legge del 2018 sulla protezione dei dati.

⁽⁸⁷⁾ Sezione 98 della legge sull'accesso ai dati e sul loro utilizzo che introduce la sezione 146, paragrafo 11 A, della legge del 2018 sulla protezione dei dati.

⁽⁸⁸⁾ Sezione 98 della legge sull'accesso ai dati e sul loro utilizzo che introduce la sezione 146, paragrafo 8B, della legge del 2018 sulla protezione dei dati.

- (66) La sezione 102 della legge sull'accesso ai dati e sul loro utilizzo introduce nuovi obblighi di presentazione di relazioni a carico dell'Information Commission. Essa modifica la sezione 139 e inserisce una nuova sezione 161 A nella legge del 2018 sulla protezione dei dati, imponendo all'Information Commission la pubblicazione di una relazione annuale sull'azione normativa. Tale relazione deve specificare come sono stati esercitati i poteri di indagine e di esecuzione derivanti dal GDPR del Regno Unito e dalle parti 3 e 4 della legge del 2018 sulla protezione dei dati. Essa deve inoltre indicare il numero di avvisi di irrogazione di sanzioni emessi oltre il termine di sei mesi a seguito di una comunicazione di avvio del procedimento e fornire le motivazioni del ritardo. La relazione deve anche spiegare in quale modo l'Information Commission ha seguito i propri orientamenti all'atto dell'adozione di decisioni normative.
- (67) La sezione 103 della legge sull'accesso ai dati e sul loro utilizzo rafforza la procedura di reclamo a disposizione degli interessati, inserendo due nuove sezioni, 164 A e 164B, nella legge del 2018 sulla protezione dei dati. La sezione 164 A stabilisce il diritto degli interessati di presentare un reclamo direttamente ai titolari del trattamento se ritengono che i diritti loro riconosciuti dal GDPR del Regno Unito o dalla parte 3 della legge del 2018 sulla protezione dei dati siano stati violati. I titolari del trattamento devono agevolare tale procedura, confermando il ricevimento del reclamo entro 30 giorni e rispondere senza indebito ritardo. Devono inoltre tenere informati i reclamanti in merito ai progressi e ai risultati. La sezione 164B conferisce al segretario di Stato il potere di adottare norme che impongono ai titolari del trattamento di segnalare il numero di reclami ricevuti.
- (68) La sezione 104 della legge sull'accesso ai dati e sul loro utilizzo inserisce nella legge del 2018 sulla protezione dei dati una nuova sezione 180 A che chiarisce le competenze dei giudici nei procedimenti per la richiesta di accesso degli interessati. In virtù di tale disposizione, i giudici possono imporre ai titolari del trattamento di fornire le informazioni controverse per poterle esaminare nell'ambito dell'adozione di una decisione in merito al diritto di accesso dell'interessato. Tuttavia le informazioni possono essere comunicate all'interessato solo se il giudice ha accertato il diritto di accedervi. Tale sezione chiarisce che i giudici possono esaminare il materiale controverso senza divulgarlo prematuramente all'attore, ripristinando una garanzia assicurata in precedenza dalla legge del 1998 sulla protezione dei dati.
- (69) Per quanto riguarda l'attuazione di tali poteri, dopo l'adozione della decisione di esecuzione (UE) 2021/1773 l'Information Commissioner ha trattato numerosi reclami⁽⁸⁹⁾, ha condotto diverse indagini e ha adottato misure di esecuzione in relazione al trattamento dei dati da parte delle autorità di contrasto. Tra il 2021 e il 2025 l'Information Commissioner ha condotto indagini e ha ammonito vari organi di polizia per diverse violazioni degli obblighi in materia di protezione dei dati, commesse ad esempio nel rispondere a richieste di accesso ai dati, nel predisporre misure di sicurezza per i dati di videosorveglianza, nel trattare informazioni giudiziali penali sensibili, nel riunire dati di persone diverse o nel divulgare dati personali a terzi⁽⁹⁰⁾. L'Information Commissioner ha inoltre pubblicato e aggiornato orientamenti, pareri e documenti di orientamento, ad esempio sul diritto di accesso o su come trattare le richieste manifestamente infondate o eccessive a norma della parte 3 della legge del 2018 sulla protezione dei dati⁽⁹¹⁾, o ha aggiornato gli orientamenti esistenti, come i suoi orientamenti relativi al trattamento dei dati a fini di contrasto⁽⁹²⁾.

3. CONCLUSIONI

- (70) La Commissione ritiene che la parte 3 della legge del 2018 sulla protezione dei dati continui ad assicurare un livello di protezione dei dati personali trasferiti per finalità di contrasto in materia penale dalle autorità competenti nell'Unione europea alle autorità competenti nel Regno Unito che è sostanzialmente equivalente a quello garantito dalla direttiva (UE) 2016/680.

⁽⁸⁹⁾ Ad esempio, nel periodo 2023-2024 l'Information Commission ha ricevuto 1 890 reclami sulla base del GDPR e/o della legge del 2018 sulla protezione dei dati, riguardanti organizzazioni rientranti nei sottosettori «autorità di polizia», «forze di polizia» e «Commissari di polizia». Cfr. anche *Information Commissioner's Annual Report and Financial Statements 2023/24*, disponibile al seguente indirizzo: <https://ico.org.uk/media2/migrated/4030348/annual-report-2023-24.pdf>.

⁽⁹⁰⁾ Ulteriori informazioni sono disponibili al seguente indirizzo: <https://ico.org.uk/action-weve-taken/enforcement/?ensector=criminal-justice>.

⁽⁹¹⁾ Disponibili al seguente indirizzo: <https://ico.org.uk/for-organisations/law-enforcement/the-right-of-access-part-3-of-the-dpa-2018/> e <https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/individual-rights/manifestly-unfounded-and-excessive-requests/>.

⁽⁹²⁾ Disponibili al seguente indirizzo: <https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/>.

- (71) Inoltre la Commissione ritiene che, nel complesso, i meccanismi di vigilanza e i mezzi di ricorso previsti dal diritto del Regno Unito continuano a consentire di individuare e sanzionare nella pratica le violazioni e offrano all'interessato mezzi di ricorso che gli permettono di accedere ai dati personali che lo riguardano e, se del caso, di ottenerne la rettifica o la cancellazione.
- (72) Di conseguenza è opportuno decidere che il Regno Unito continua ad assicurare un livello di protezione adeguato ai sensi dell'articolo 36, paragrafo 2, della direttiva (UE) 2016/680, interpretato alla luce della Carta dei diritti fondamentali dell'Unione europea.

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

- (73) Gli Stati membri e i loro organi sono tenuti ad adottare le misure necessarie per conformarsi agli atti delle istituzioni dell'Unione, poiché questi ultimi si presumono legittimi e producono pertanto effetti giuridici finché non scadano, non siano stati revocati o annullati nel contesto di un ricorso per annullamento ovvero dichiarati invalidi a seguito di un rinvio pregiudiziale o di un'eccezione di illegittimità.
- (74) Di conseguenza, una decisione di adeguatezza adottata dalla Commissione a norma dell'articolo 36, paragrafo 3, della direttiva (UE) 2016/680 è vincolante per tutti gli organi degli Stati membri che ne sono destinatari, comprese le autorità di controllo indipendenti. In particolare, durante il periodo di applicazione della decisione di esecuzione (UE) 2021/1773, come modificata dalla presente decisione, i trasferimenti da un titolare del trattamento o un responsabile del trattamento nell'Unione verso titolari del trattamento o responsabili del trattamento nel Regno Unito possono avvenire senza la necessità di ottenere ulteriori autorizzazioni.
- (75) Allo stesso tempo è opportuno ricordare che, ai sensi dell'articolo 47, paragrafo 5, della direttiva (UE) 2016/680, e come spiegato dalla Corte di giustizia nella sentenza *Schrems I*, quando un'autorità nazionale di protezione dei dati mette in dubbio, anche in seguito a un reclamo, la compatibilità di una decisione di adeguatezza della Commissione con i diritti fondamentali della persona fisica concernenti la tutela della vita privata e la protezione dei dati, il diritto nazionale deve prevedere mezzi di ricorso che consentano di far valere tali obiezioni dinanzi a un organo giurisdizionale nazionale, che può essere tenuto a effettuare un rinvio pregiudiziale alla Corte di giustizia (93).

5. MONITORAGGIO

- (76) Ai sensi dell'articolo 36, paragrafo 4, della direttiva (UE) 2016/680, la Commissione è tenuta a monitorare, su base continuativa, gli sviluppi pertinenti nel Regno Unito al fine di valutare se sia sempre assicurato un livello essenzialmente equivalente di protezione. Tale monitoraggio è particolarmente importante perché il Regno Unito applicherà e farà rispettare un regime modificato di protezione dei dati. Inoltre il quadro modificato del Regno Unito in materia di protezione dei dati conferisce al segretario di Stato il potere di specificare ulteriormente tale quadro mediante atti di diritto derivato. A tale riguardo, occorre prestare particolare attenzione a tali specifiche supplementari nonché all'applicazione pratica delle norme modificate del Regno Unito sui trasferimenti di dati personali verso paesi terzi, all'efficacia dell'esercizio dei diritti individuali, compresi eventuali sviluppi pertinenti del diritto e delle prassi riguardanti le nuove eccezioni o limitazioni a tali diritti, e al funzionamento dell'ICO ristrutturato, anche per quanto riguarda la gestione dei reclami e l'applicazione dei poteri correttivi. Assieme ad altri elementi, gli sviluppi giurisprudenziali e la vigilanza da parte dell'ICO e di altri organismi indipendenti dovrebbero contribuire al monitoraggio della Commissione.
- (77) Per agevolare tale monitoraggio, le autorità del Regno Unito dovrebbero informare tempestivamente e regolarmente la Commissione di qualsiasi modifica sostanziale dell'ordinamento giuridico del Regno Unito che abbia un impatto sul quadro giuridico oggetto della decisione di esecuzione (UE) 2021/1773, come modificata dalla presente decisione, nonché di qualsiasi evoluzione delle pratiche relative al trattamento dei dati personali oggetto della decisione di esecuzione (UE) 2021/1773, come modificata dalla presente decisione, in particolare per quanto riguarda gli elementi di cui al considerando (39).
- (78) Inoltre, al fine di consentire alla Commissione di svolgere in modo efficace la propria funzione di monitoraggio, gli Stati membri dovrebbero informarla delle eventuali azioni intraprese dalle autorità nazionali di protezione dei dati, in particolare per quanto riguarda eventuali domande o reclami presentati da interessati dell'UE relativamente al trasferimento di dati personali dall'Unione europea verso autorità competenti nel Regno Unito. La Commissione dovrebbe inoltre essere informata di eventuali indicazioni del fatto che le azioni delle autorità pubbliche del Regno Unito competenti a fini di prevenzione, indagine, accertamento e perseguitamento di reati, compresi gli organismi di vigilanza, non garantiscono il necessario livello di protezione.

(93) *Schrems I*, punto 65.

- (79) Se dalle informazioni disponibili, in particolare da quelle risultanti dal monitoraggio della presente decisione o fornite dalle autorità del Regno Unito o degli Stati membri, risulta che il livello di protezione offerto dal Regno Unito potrebbe non essere più adeguato, la Commissione dovrebbe informare prontamente le autorità competenti del Regno Unito e richiedere che adottino misure adeguate entro un periodo di tempo specificato, che non può essere superiore a tre mesi. Se necessario, tale periodo può essere prorogato per un periodo di tempo determinato, tenuto conto della natura della questione in esame e/o delle misure da adottare.
- (80) Laddove alla scadenza di tale periodo di tempo specificato le autorità competenti del Regno Unito non abbiano adottato tali misure o non dimostrino altrimenti in modo soddisfacente che la presente decisione continua ad essere basata su un livello di protezione adeguato, la Commissione avvierà la procedura di cui all'articolo 58, paragrafo 2, della direttiva (UE) 2016/680 al fine di sospendere o abrogare parzialmente o completamente la presente decisione.
- (81) In alternativa, la Commissione avvierà tale procedura al fine di modificare la decisione di esecuzione (UE) 2021/1773, come modificata dalla presente decisione, in particolare imponendo ulteriori condizioni per i trasferimenti di dati o limitando il riconoscimento dell'adeguatezza soltanto ai trasferimenti di dati per cui continua ad essere garantito un livello di protezione adeguato.
- (82) In ragione di motivi imperativi d'urgenza debitamente giustificati, la Commissione farà ricorso alla possibilità di adottare, conformemente alla procedura di cui all'articolo 58, paragrafo 3, della direttiva (UE) 2016/680, atti di esecuzione immediatamente applicabili destinati a sospendere, abrogare o modificare la presente decisione.

6. RIESAME, DURATA E RINNOVO DELLA PRESENTE DECISIONE

- (83) In applicazione dell'articolo 36, paragrafo 3, della direttiva (UE) 2016/680 e alla luce del fatto che il livello di protezione assicurato dal quadro giuridico del Regno Unito può evolversi, la Commissione, successivamente all'adozione della presente decisione, dovrebbe riesaminare periodicamente se le constatazioni relative al livello di protezione assicurato dal Regno Unito continuano ad essere giustificate in fatto e in diritto. Tali valutazioni dovrebbero aver luogo almeno ogni quattro anni e dovrebbero riguardare tutti gli aspetti del funzionamento della presente decisione, compreso il funzionamento dei pertinenti meccanismi di controllo e applicazione.
- (84) Per effettuare il riesame, la Commissione dovrebbe incontrare i rappresentanti pertinenti delle autorità britanniche, compresa l'Information Commission. A tale riunione dovrebbero poter partecipare i rappresentanti dei membri del comitato europeo per la protezione dei dati. Nel quadro del riesame la Commissione dovrebbe chiedere al Regno Unito di fornire informazioni complete su tutti gli aspetti pertinenti alla constatazione di adeguatezza. La Commissione dovrebbe inoltre chiedere delucidazioni in merito a qualsiasi informazione ricevuta risultata pertinente ai fini della presente decisione, compreso dall'EDPB, dalle singole autorità di protezione dei dati e dai gruppi della società civile, da relazioni pubbliche o dalle notizie diffuse dai mezzi di comunicazione o da qualsiasi altra fonte di informazioni disponibile.
- (85) La Commissione dovrebbe elaborare, sulla base del riesame, una relazione pubblica da presentare al Parlamento europeo e al Consiglio.
- (86) La Commissione deve anche tenere conto del fatto che il quadro in materia di protezione dei dati valutato nella presente decisione e nella decisione di esecuzione (UE) 2021/1773 può evolvere ulteriormente.
- (87) Di conseguenza è opportuno prevedere che la presente decisione si applichi per un periodo di sei anni a decorrere dalla sua entrata in vigore.
- (88) Laddove in particolare le informazioni risultanti dal monitoraggio della presente decisione rivelino che le conclusioni sull'adeguatezza del livello di protezione assicurato nel Regno Unito continuano ad essere giustificate in fatto e in diritto, la Commissione dovrebbe, al più tardi sei mesi prima della data in cui la presente decisione cesserà di applicarsi, avviare la procedura per modificare la presente decisione prorogandone l'applicazione temporale, in linea di principio, per un ulteriore periodo di quattro anni. Qualsiasi atto di esecuzione di tale sorta destinato a modificare la presente decisione deve essere adottato conformemente alla procedura di cui all'articolo 58, paragrafo 2, della direttiva (UE) 2016/680.

7. CONSIDERAZIONI FINALI

- (89) Il comitato europeo per la protezione dei dati ha pubblicato un parere⁽⁹⁴⁾, del quale si è tenuto conto nell'elaborazione della presente decisione.
- (90) La misura di cui alla presente decisione è conforme al parere del comitato istituito a norma dell'articolo 58 della direttiva (UE) 2016/680.
- (91) A norma dell'articolo 6 *bis* del protocollo n. 21 sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al TUE e al TFUE, l'Irlanda non è vincolata dalle disposizioni previste dalla direttiva (UE) 2016/680, e di conseguenza dalla presente decisione di esecuzione, che riguardano il trattamento dei dati personali da parte degli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione della parte terza, titolo V, capi 4 o 5, TFUE laddove l'Irlanda non sia vincolata da norme che disciplinano forme di cooperazione giudiziaria in materia penale o di cooperazione di polizia nell'ambito delle quali devono essere rispettate le disposizioni stabilite in base all'articolo 16 TFUE. Ciononostante, in virtù della decisione di esecuzione (UE) 2020/1745 del Consiglio⁽⁹⁵⁾, la direttiva (UE) 2016/680 è messa in applicazione e si applica in Irlanda in via provvisoria a decorrere dal 1º gennaio 2021. L'Irlanda è pertanto vincolata dalla presente decisione, alle stesse condizioni applicabili all'applicazione della direttiva (UE) 2016/680 in Irlanda come stabilito nella decisione di esecuzione (UE) 2020/1745, per quanto concerne la parte dell'acquis di Schengen alla quale partecipa.
- (92) Conformemente agli articoli 2 e 2 *bis* del protocollo n. 22 sulla posizione della Danimarca, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, la Danimarca non è vincolata dalle disposizioni previste dalla direttiva (UE) 2016/680, e di conseguenza dalla presente decisione di esecuzione, né soggetta alla loro applicazione per quanto concerne il trattamento di dati personali da parte degli Stati membri durante lo svolgimento di attività che rientrano nell'ambito di applicazione della parte terza, titolo V, capi 4 o 5, TFUE. Tuttavia, dato che la direttiva (UE) 2016/680 si basa sull'acquis di Schengen, il 26 ottobre 2016 la Danimarca, conformemente all'articolo 4 di tale protocollo, ha notificato la propria decisione di attuare la direttiva (UE) 2016/680. La Danimarca è pertanto tenuta ad attuare la presente decisione in virtù del diritto internazionale.
- (93) Per quanto riguarda l'Islanda e la Norvegia, la presente decisione costituisce uno sviluppo delle disposizioni dell'acquis di Schengen ai sensi dell'accordo concluso dal Consiglio dell'Unione europea con la Repubblica d'Islanda e il Regno di Norvegia sulla loro associazione all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen⁽⁹⁶⁾.
- (94) Per quanto riguarda la Svizzera, la presente decisione costituisce uno sviluppo delle disposizioni dell'acquis di Schengen ai sensi dell'accordo tra l'Unione europea, la Comunità europea e la Confederazione svizzera, riguardante l'associazione della Confederazione svizzera all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen⁽⁹⁷⁾.
- (95) Per quanto riguarda il Liechtenstein, la presente decisione costituisce uno sviluppo delle disposizioni dell'acquis di Schengen ai sensi del protocollo tra l'Unione europea, la Comunità europea, la Confederazione svizzera e il Principato del Liechtenstein sull'adesione del Principato del Liechtenstein all'accordo tra l'Unione europea, la Comunità europea e la Confederazione svizzera riguardante l'associazione della Confederazione svizzera all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen⁽⁹⁸⁾.
- (96) È pertanto opportuno modificare di conseguenza la decisione di esecuzione (UE) 2021/1773,

⁽⁹⁴⁾ Parere 27/2025 relativo al progetto di decisione di esecuzione della Commissione europea sull'adeguata protezione dei dati personali da parte del Regno Unito, disponibile al seguente indirizzo: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-272025-regarding-european-commission-draft_it.

⁽⁹⁵⁾ Decisione di esecuzione (UE) 2020/1745 del Consiglio, del 18 novembre 2020, relativa alla messa in applicazione delle disposizioni dell'acquis di Schengen in materia di protezione dei dati e all'applicazione provvisoria di talune disposizioni dell'acquis di Schengen in Irlanda (GU L 393 del 23.11.2020, pag. 3, ELI: http://data.europa.eu/eli/dec_impl/2020/1745/oj).

⁽⁹⁶⁾ Accordo concluso dal Consiglio dell'Unione europea con la Repubblica d'Islanda e il Regno di Norvegia sulla loro associazione all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen (GU L 176 del 10.7.1999, pag. 36, ELI: [http://data.europa.eu/eli/agree_internation/1999/439\(1\)/oj](http://data.europa.eu/eli/agree_internation/1999/439(1)/oj)).

⁽⁹⁷⁾ GU L 53 del 27.2.2008, pag. 52.

⁽⁹⁸⁾ GU L 160 del 18.6.2011, pag. 21.

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

L'articolo 4 della decisione di esecuzione (UE) 2021/1773 è sostituito dal seguente:

«Articolo 4

La presente decisione scade il 27 dicembre 2031, a meno che non sia prorogata secondo la procedura di cui all'articolo 58, paragrafo 2, della direttiva (UE) 2016/680.»

Articolo 2

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 19 dicembre 2025

Per la Commissione
Michael MCGRATH
Membro della Commissione
