2025/2571

23.12.2025

DECISIÓN DE EJECUCIÓN (UE) 2025/2571 DE LA COMISIÓN

de 19 de diciembre de 2025

por la que se modifica la Decisión de Ejecución (UE) 2021/1773 de la Comisión con arreglo a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por parte del Reino Unido

[notificada con el número C(2025) 8782]

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Vista la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (Directiva sobre protección de datos en el ámbito penal) ([1]), y en particular su artículo 36, apartado 3,

Considerando lo siguiente:

1. INTRODUCCIÓN

(1) Mediante la Decisión de Ejecución (UE) 2021/1773 de la Comisión ([2]) se concluye que, a efectos del artículo 36 de la Directiva (UE) 2016/680, el Reino Unido garantiza un nivel adecuado de protección para los datos personales transferidos, dentro del ámbito de aplicación de dicha Directiva, desde la Unión Europea al Reino Unido.

(2) Al adoptar la Decisión de Ejecución (UE) 2021/1773, la Comisión tuvo en cuenta que, al final del período transitorio establecido en el Acuerdo sobre la retirada del Reino Unido de Gran Bretaña e Irlanda del Norte de la Unión Europea y de la Comunidad Europea de la Energía Atómica ([3]) y una vez que la disposición provisional del artículo 782 del Acuerdo de Comercio y Cooperación entre la Unión Europea y la Comunidad Europea de la Energía Atómica, por una parte, y el Reino Unido de Gran Bretaña e Irlanda del Norte, por otra ([4]), hubiera dejado de aplicarse, el Reino Unido puede adoptar, aplicar y hacer cumplir un nuevo régimen de protección de datos distinto del vigente cuando estaba vinculado por el Derecho de la Unión.

(3) Dado que estas circunstancias pueden haber supuesto modificaciones del marco de protección de datos evaluado en la Decisión de Ejecución (UE) 2021/1773 u otros cambios pertinentes, se consideró apropiado establecer que dicha Decisión se aplicaría durante un período de cuatro años a partir de su entrada en vigor. La Decisión de Ejecución (UE) 2021/1773 dejaba de tener validez el 27 de junio de 2025, salvo que se prorrogase de conformidad con el procedimiento indicado en el artículo 58, apartado 2, de la Directiva (UE) 2016/680.

(4) Para decidir si procede la prórroga de la Decisión de Ejecución (UE) 2021/1773, la Comisión debe evaluar si la conclusión de que el Reino Unido garantiza un nivel adecuado de protección sigue estando justificada de hecho y de Derecho, habida cuenta de los cambios acaecidos desde la adopción de la Decisión de Ejecución (UE) 2021/1773 con respecto a los elementos enumerados en el artículo 36, apartado 2, de la Directiva (UE) 2016/680.

(5) En particular, el 23 de octubre de 2024, el Gobierno del Reino Unido presentó al Parlamento del Reino Unido el Data (Use and Access) Bill ([5]) [proyecto de Ley sobre datos (uso y acceso)], con el que se modificaba la Data Protection Act [Ley de protección de datos] de 2018 (DPA de 2018), evaluada en la Decisión de Ejecución

([1]) DO L 119 de 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj.
([2]) Decisión de Ejecución (UE) 2021/1773 de la Comisión, de 28 de junio de 2021, con arreglo a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por parte del Reino Unido (DO L 360 de 11.10.2021, p. 69, ELI: http://data.europa.eu/eli/dec_impl/2021/1773/oj).
([3]) DO C 384 I de 12.11.2019, p. 1.
([4]) DO L 149 de 30.4.2021, p. 10, ELI: http://data.europa.eu/eli/agree_internation/2021/689(1)/oj.
([5]) Puede consultarse en el enlace siguiente (documento en inglés): https://bills.parliament.uk/bills/3825/news.

(UE) 2021/1773. El 24 de junio de 2025, la Comisión adoptó la Decisión de Ejecución (UE) 2025/1225 de la Comisión ([6]), que prorrogaba la validez de la Decisión (UE) 2021/1773 por un período de seis meses, hasta el 27 de diciembre de 2025. Esta prórroga técnica de duración limitada permitió a la Comisión concluir su evaluación para determinar si el nivel de protección de los datos personales garantizado por el Reino Unido sobre la base de un marco jurídico estable es adecuado, esto es, tras la finalización del expediente legislativo en curso.

(6) Tras la adopción de la Decisión de Ejecución (UE) 2021/1773, la Comisión supervisó de forma permanente los acontecimientos pertinentes en el Reino Unido ([7]). De conformidad con el considerando 165 de la Decisión de Ejecución (UE) 2021/1773, se prestó especial atención a la aplicación práctica de las normas del Reino Unido relativas a las transferencias de datos personales a terceros países y al impacto que pueda tener en el nivel de protección que se garantiza a los datos transferidos en virtud de dicha Decisión; a la eficacia del ejercicio de los derechos individuales, en particular a cualquier avance pertinente en la legislación y en la práctica con respecto a las excepciones o limitaciones de dichos derechos. La supervisión de la Comisión se basó en, entre otros elementos, los avances de la jurisprudencia y la supervisión de la Information Commissioner's Office [Oficina del Comisionado de Información] (ICO) y otros organismos independientes.

(7) Basándose en la evaluación de estos acontecimientos, también de las modificaciones de la DPA de 2018 introducidas por la Data (Use and Access) Act [Ley de datos (uso y acceso)], la Comisión concluye que el Reino Unido sigue garantizando un nivel adecuado de protección para los datos personales transferidos dentro del ámbito de aplicación de la Directiva (UE) 2016/680 de la Unión Europea al Reino Unido.

2. CAMBIOS IMPORTANTES EN LAS NORMAS APLICABLES AL TRATAMIENTO DE DATOS PERSONALES

2.1. El marco de protección de datos del Reino Unido

(8) Cuando se adoptó la Decisión de Ejecución (UE) 2021/1773, el marco jurídico para el tratamiento de datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública en el Reino Unido, consistía en las partes pertinentes de la DPA de 2018 ([8]), en su versión modificada por la normativa Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (DPPEC Regulations) ([9]) [Reglamentos en materia de protección de datos, privacidad y comunicaciones electrónicas (modificaciones, etc.) (salida de la UE) de 2019], y más concretamente en la parte 3 de dicha ley.

(9) Si bien esta ley, que reflejaba fielmente las normas correspondientes aplicables en la Unión Europea, sigue conformando la legislación en materia de protección de datos del Reino Unido para las actividades de tratamiento pertinentes, desde entonces ha sido objeto de un número limitado de modificaciones, lo que constata que el Reino Unido ya no está sujeto al Derecho de la Unión Europea.

(10) En primer lugar, la Retained EU Law (Revocation and Reform) Act [Ley sobre el Derecho de la Unión conservado (revocación y reforma)] de 2023 (REUL Act) ([10]) aclaró que los principios generales del Derecho de la Unión ya no formaban parte del Derecho interno del Reino Unido después de finales de 2023 ([11]). Por otra parte, los tribunales del Reino Unido ya no están obligados a interpretar el «Derecho asimilado» no modificado, que anteriormente se

([6]) Decisión de Ejecución (UE) 2025/1225 de la Comisión, de 24 de junio de 2025, por la que se modifica la Decisión de Ejecución (UE) 2021/1773 con arreglo a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por parte del Reino Unido (DO L, 2025/1225, 26.6.2025, ELI: http://data.europa.eu/eli/dec_impl/2025/1225/oj).

([7]) Artículo 36, apartado 4, de la Directiva (UE) 2016/680.

([8]) La Data Protection Act de 2018 puede consultarse en el enlace siguiente (documento en inglés): https://www.legislation.gov.uk/ukpga/2018/12/contents. Antes de la retirada del Reino Unido de la Unión Europea y durante el período transitorio, la DPA de 2018 estableció normas nacionales, cuando lo permitía el Reglamento (UE) 2016/679, que especificaban y restringían las normas del Reglamento (UE) 2016/679, y la Directiva transpuesta (UE) 2016/680.

([9]) La normativa Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations de 2019, puede consultarse en el siguiente enlace (documento en inglés): https://www.legislation.gov.uk/uksi/2019/419/contents/made, y en su versión modificada por la normativa DPPEC Regulations de 2020, disponible en el siguiente enlace (documento en inglés): https://www.legislation.gov.uk/ukdsi/2020/9780348213522. La normativa DDPEC Regulations modifica el Reglamento (UE) 2016/679 incorporado a la legislación del Reino Unido a través de la European Union (Withdrawal) Act de 2018, la DPA de 2018 y otra legislación en materia de protección de datos a fin de adaptarlo al contexto nacional.

([10]) Retained EU Law (Revocation and Reform) Act 2023 [Ley sobre el Derecho de la Unión conservado (revocación y reforma)] de 2023, disponible en el siguiente enlace: https://www.legislation.gov.uk/ukpga/2023/28.

([11]) Sección 5 de la European Union (Withdrawal) Act de 2018, en su versión modificada por la REUL Act.

denominaba «Derecho de la Unión conservado», de conformidad con los principios generales del Derecho de la Unión, sino que dicho Derecho debe interpretarse de manera compatible con el Derecho interno del Reino Unido ([12]). Sin embargo, los tribunales competentes del Reino Unido todavía deben interpretar el Derecho asimilado no modificado de conformidad con la jurisprudencia pertinente del Tribunal de Justicia de la Unión Europea dictada antes del final del período transitorio ([13]), como también se menciona en el considerando 12 de la Decisión de Ejecución (UE) 2021/1773. La DPA de 2018 ha sido modificada por la Data (Use and Access) Act [Ley sobre datos (uso y acceso)] para aclarar el efecto de la REUL Act en la legislación del Reino Unido en materia de protección de datos. Por ejemplo, la sección 183A, apartado 1, de la DPA de 2018 establece como norma general que toda nueva legislación (aprobada a partir del 20 de agosto de 2025) que introduzca nuevas obligaciones o competencias para tratar datos personales se presume sujeta a la legislación del Reino Unido en materia de protección de datos. Esto significa que el marco de protección de datos del Reino Unido sigue prevaleciendo sobre otra legislación. De conformidad con la sección 183A, apartado 2, letra b), de la DPA de 2018, esta presunción puede dejar de aplicarse si el Parlamento del Reino Unido decide deliberadamente hacerlo de manera expresa en la legislación, preservando la soberanía parlamentaria. Además, la sección 186, apartado 2A, de la DPA de 2018 aclara que las limitaciones a los derechos de los interesados enumeradas en la sección 186, apartado 3, de la DPA de 2018 no quedan invalidadas por la sección 186, apartado 1, de la DPA de 2018, que establece que las disposiciones que prohíben o restringen la divulgación de información no prevalecen sobre determinados derechos de protección de datos. Esto garantiza que, por ejemplo, las restricciones a los derechos de los interesados establecidas en la DPA de 2018 no entren en el ámbito de aplicación de la «anulación de la protección de datos» general de la sección 186, apartado 1, de la DPA de 2018.

(11) En segundo lugar, desde la adopción de la Decisión de Ejecución (UE) 2021/1773, la legislación en materia de protección de datos del Reino Unido ha sido modificada por la normativa Data Protection (Fundamental Rights and Freedoms) (Amendment) Regulations [Reglamentos de modificación en materia de protección de datos (derechos y libertades fundamentales)] de 2023 ([14]). Dicha normativa define las referencias a los derechos fundamentales o las libertades fundamentales incluidas en la DPA de 2018 (que se habían definido previamente para incluir los derechos fundamentales y las libertades fundamentales de la UE ([15])) como las referencias a los derechos consagrados en el Convenio Europeo de Derechos Humanos (CEDH), aplicados en el Derecho interno del Reino Unido a través de la Human Rights Act (Ley de derechos humanos) de 1998 ([16]). La Human Rights Act, de 1998, incorpora al Derecho del Reino Unido los derechos recogidos en el Convenio Europeo de Derechos Humanos. La Human Rights Act concede a toda persona los derechos y libertades fundamentales recogidos en los artículos 2 a 12 y 14 del Convenio Europeo de Derechos Humanos, los artículos 1 a 3 de su Protocolo n.º 1 y el artículo 1 de su Protocolo n.º 13, leídos en relación con los artículos 16, 17 y 18 de dicho Convenio. Esto incluye el derecho al respeto a la vida privada y familiar (y el derecho a la protección de los datos como parte del anterior derecho), así como el derecho a un proceso equitativo ([17]).

(12) Por último, la DPA de 2018 ha sido objeto de reformas específicas previstas en las partes 5 y 6 de la Data (Use and Access) Act. Si bien el ámbito de aplicación de esta va mucho más allá de la protección de los datos personales, prevé un número limitado de modificaciones de varios aspectos del régimen de protección de datos tales como, entre otros, las modalidades de ejercicio de los derechos de los interesados, las condiciones de las decisiones automatizadas, así como el alcance de determinados requisitos de rendición de cuentas. Además, la Data (Use and Access) Act [Ley sobre datos (uso y acceso)] introduce modificaciones en la estructura de gobernanza de la ICO. Una vez aplicadas, estas medidas sustituirán a la ICO por una nueva entidad, la Information Commission [Comisión de Información]. El papel y las funciones del regulador como autoridad independiente de control de la protección de datos en el Reino Unido se mantendrán sin cambios. La Ley también introduce nuevas competencias de ejecución para el regulador.

(13) La presente Decisión evalúa los avances legislativos, reglamentarios y de otra índole pertinentes para la conclusión sobre el nivel de protección garantizado por el Reino Unido expuesta en la Decisión de Ejecución (UE) 2021/1773. La evaluación llevada a cabo mediante la Decisión de Ejecución (UE) 2021/1773 sigue siendo válida en lo que respecta a aquellos aspectos del marco de protección de datos del Reino Unido que no han sido modificados ni se han visto afectados por otros acontecimientos desde la adopción de dicha Decisión de Ejecución.

([12]) Sección 5(A2) de la European Union (Withdrawal) Act de 2018, en su versión modificada por la REUL Act.
([13]) Sección 6, apartados 3 y 7, de la European Union Withdrawal Act de 2018, en su versión modificada por la REUL Act.
([14]) Puede consultarse en el enlace siguiente (documento en inglés): https://www.gov.uk/government/publications/the-data-protection-fundamental-rights-and-freedoms-amendment-regulations-2023.
([15]) Los derechos fundamentales y las libertades fundamentales de la UE se habían mantenido en el Derecho del Reino Unido a través de la sección 4 de la European Union (Withdrawal) Act de 2018, que fue derogada a finales de 2023 por la REUL Act.
([16]) Sección 2, apartado 3, de la normativa Data Protection (Fundamental Rights and Freedoms) Amendment Regulations de 2023.
([17]) Artículos 6, 8, 10 y 13 del Convenio Europeo de Derechos Humanos (véase también el anexo 1 de la Human Rights Act, de 1998, disponible en el siguiente enlace: https://www.legislation.gov.uk/ukpga/1998/42/contents).

(14) Los avances legislativos, reglamentarios y de otra índole pertinentes se analizan en profundidad en las siguientes secciones sobre la base del principio de adecuación, según el cual la Comisión debe determinar si el tercer país en cuestión garantiza un nivel de protección «esencialmente equivalente» al que se garantiza en el contexto de la Unión ([18]). Tal como ha precisado el Tribunal de Justicia de la Unión Europea, no se exige un nivel de protección idéntico ([19]). En particular, los medios de que se sirve el tercer país en cuestión para la protección de los datos personales pueden ser diferentes de los aplicados en la Unión Europea, siempre que, en la práctica, sean eficaces para garantizar un nivel de protección adecuado ([20]). Por consiguiente, el principio de adecuación no exige que se reproduzcan al pie de la letra las normas de la Unión, sino que el criterio radica en si, a través de la esencia de los derechos de privacidad y su aplicación, fuerza ejecutiva y supervisión efectivas, el ordenamiento jurídico en cuestión ofrece, en su conjunto, el nivel de protección exigido ([21]).

2.1.1. *Definiciones*

(15) El régimen de protección de datos del Reino Unido sigue aplicando conceptos básicos de la protección de datos que reflejan la terminología de la Directiva (UE) 2016/680. Estos conceptos se han evaluado en los considerandos 26 y 27 de la Decisión de Ejecución (UE) 2021/1773.

(16) En particular, al establecer la definición y las condiciones para la obtención del consentimiento del interesado, la Data (Use and Access) Act confirma cuál es el marco jurídico que rige el uso del consentimiento del interesado como una base lícita para el tratamiento de los datos personales ([22]). Las disposiciones actualizadas reproducen el lenguaje del RGPD del Reino Unido, aumentando así la coherencia entre los regímenes de protección de datos del Reino Unido. Esta armonización facilita una interpretación más clara por parte de las autoridades competentes a la hora de basarse en el consentimiento como base legal para el tratamiento.

(17) En primer lugar, la sección 69 de la Data (Use and Access) Act introduce una nueva subsección 33, apartado 1A, en la DPA de 2018, en la que se define el «consentimiento del interesado» como una manifestación de voluntad libre, específica, informada e inequívoca del interesado. Esta manifestación debe plasmarse en una declaración o una clara acción afirmativa y debe expresar la aceptación, por parte del interesado, del tratamiento de sus datos personales.

(18) En segundo lugar, esa misma sección incorpora una nueva sección 40A a la DPA de 2018, en la que se establecen las condiciones que deben cumplirse para basarse en el consentimiento del interesado. El responsable del tratamiento debe ser capaz de demostrar que el interesado ha dado un consentimiento válido. Cuando el consentimiento del interesado se obtenga por escrito dentro de un documento más amplio, debe presentarse de un modo en que se diferencie claramente de otros asuntos, utilizando un lenguaje accesible, comprensible y sencillo. No se considerará vinculante ninguna disposición del documento que incumpla estas normas ([23]).

(19) Asimismo, los responsables o los encargados del tratamiento deben informar a la persona afectada, antes de obtener el consentimiento, de su derecho a retirarlo. El proceso para retirar el consentimiento debe ser tan sencillo como el proceso para darlo. Con ello se garantiza que el interesado mantiene un control verdadero sobre el uso de sus datos personales en todo momento ([24]).

(20) Por último, la Data (Use and Access) Act aclara que a la hora de evaluar si el consentimiento del interesado «se ha dado libremente», es necesario tener en cuenta si la prestación de un servicio estaba supeditada a que el interesado autorizara el tratamiento de datos personales que no eran necesarios para la prestación de dicho servicio, lo que, de confirmarse, socavaría la validez de dicho consentimiento ([25]).

([18]) Considerando 67 de la Directiva (UE) 2016/680.
([19]) Asunto C-362/14, Maximillian Schrems/Data Protection Commissioner («Schrems I»), ECLI:EU:C:2015:650, apartado 73.
([20]) Schrems I, apartado 74.
([21]) Véase la Comunicación de la Comisión al Parlamento Europeo y al Consejo titulada «Intercambio y protección de los datos personales en un mundo globalizado», de 10 de enero de 2017, sección 3.1, pp. 6-7 [COM(2017) 7], que puede consultarse en el enlace siguiente: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52017DC0007.
([22]) Secciones 33 y 40A de la DPA de 2018, introducidas por la sección 69, apartados 1, 2 y 4, de la Data (Use and Access) Act.
([23]) Sección 40A, apartados 2 y 3, de la DPA de 2018, introducidos por la sección 69, apartado 4, de la Data (Use and Access) Act.
([24]) Sección 40A, apartados 5 y 6, de la DPA de 2018, introducidos por la sección 69, apartado 4, de la Data (Use and Access) Act.
([25]) Sección 40A, apartado 7, de la DPA de 2018, introducido por la sección 69, apartado 4, de la Data (Use and Access) Act.

(21) Es importante señalar que, con arreglo a la parte 3 revisada de la DPA de 2018, el consentimiento del interesado sigue sin ser un fundamento jurídico pertinente para las operaciones de tratamiento contempladas en el ámbito de aplicación de la presente Decisión, como se explica en el considerando 35 de la Decisión de Ejecución (UE) 2021/1773. Además, como se observa en el considerando 36 de esa misma Decisión de Ejecución, en un contexto de aplicación de la ley, el tratamiento sigue sin ser posible basándose únicamente en el consentimiento del interesado, dado que una autoridad competente debe estar siempre investida de un poder que le permita tratar los datos. En concreto, y de manera similar a lo permitido por la Directiva (UE) 2016/680 ([26]), esto significa que el consentimiento del interesado sirve como condición adicional para permitir ciertas operaciones limitadas y específicas de tratamiento que, de otro modo, no podrían llevarse a cabo como, por ejemplo, la recogida y el tratamiento de una muestra de ADN de un individuo que no es sospechoso.

2.2. **Garantías, derechos y obligaciones**

2.2.1. *Tratamiento de datos personales sensibles*

(22) El marco de protección de datos del Reino Unido sigue previendo garantías específicas cuando intervienen categorías especiales de datos, como se evalúa en los considerandos 38 a 42 de la Decisión de Ejecución (UE) 2021/1773.

(23) En la parte 3 de la DPA de 2018 siguen vigentes tanto la definición de las categorías especiales de datos personales como las normas específicas aplicables al tratamiento de dichas categorías. Al mismo tiempo, la Data (Use and Access) Act confiere nuevos poderes normativos al secretario de Estado para incorporar nuevas categorías especiales de datos y adaptar las condiciones aplicables a su utilización, si fuera necesario ([27]). Es importante señalar que estos poderes no permiten al secretario de Estado suprimir ni modificar ninguna categoría especial de datos existente, ni tampoco alterar las condiciones aplicables al tratamiento de dichas categorías ([28]).

(24) Por consiguiente, estas modificaciones no afectan al nivel de protección de las categorías especiales de datos personales considerado esencialmente equivalente al nivel que otorga en la UE la Decisión de Ejecución (UE) 2021/1773.

2.2.2. *Derechos individuales*

(25) En el ordenamiento jurídico del Reino Unido, los interesados siguen gozando de los mismos derechos individuales que los previstos en la Directiva (UE) 2016/680, los cuales pueden hacer valer ante el responsable o el encargado del tratamiento, en concreto el derecho de acceso a los datos, el derecho a oponerse al tratamiento y el derecho de rectificación o supresión de datos, tal como se evalúa en los considerandos 57 a 65 de la Decisión de Ejecución (UE) 2021/1773.

(26) La Data (Use and Access) Act aclara una serie de modalidades concretas en virtud de las cuales pueden ejercerse dichos derechos.

(27) En primer lugar, conforme al régimen en vigor, los responsables del tratamiento tienen derecho a rechazar una solicitud o a cobrar una tasa razonable si una solicitud es manifiestamente infundada o excesiva ([29]). A este respecto, la Data (Use and Access) Act confiere un nuevo poder normativo al secretario de Estado, en virtud del cual este puede emitir normativa que obligue a los responsables del tratamiento a elaborar y publicar orientaciones sobre las tasas que cobran en tales circunstancias. Por otro lado, cuando los responsables del tratamiento se niegan a atender una solicitud aludiendo a los motivos antes señalados, la Data (Use and Access) Act aclaró que siguen teniendo la obligación de informar al interesado de los motivos de la denegación y de su derecho a presentar una reclamación ante el Information Commissioner [Comisionado de Información]. Dicha información debe transmitirse sin dilación indebida ([30]).

(28) En segundo lugar, la Data (Use and Access) Act establece los plazos en los que los responsables del tratamiento deben responder a las solicitudes de los interesados. Más concretamente, ajusta los períodos de respuesta requeridos a los establecidos en el Reglamento General de Protección de Datos (RGPD) del Reino Unido. Las disposiciones revisadas también prevén una ampliación del período de respuesta de hasta dos meses adicionales cuando se trate de una

([26]) Véanse los considerandos 35 y 37 de la Directiva (UE) 2016/680.

([27]) Sección 74 de la Data (Use and Access) Act. Dicha normativa está sujeta al procedimiento de resolución afirmativa, es decir, requerirá la aprobación activa del Parlamento del Reino Unido.

([28]) Véase la nueva sección 42A de la DPA de 2018, introducida por la sección 74 de la Data (Use and Access) Act, así como las notas explicativas del Data (Use and Access) Bill [proyecto de Ley sobre datos (uso y acceso)], apartado 577, disponibles en el siguiente enlace: https://publications.parliament.uk/pa/bills/cbill/59-01/0179/en/240179en.pdf.

([29]) Artículo 53, apartado 1, de la DPA de 2018. Véase también el considerando 64 de la Decisión de Ejecución (UE) 2021/1773.

([30]) Sección 53, apartados 4A, 6 y 7, de la DPA de 2018, introducidos por la sección 75 de la Data (Use and Access) Act.

solicitud compleja o se reciban múltiples solicitudes. En tales casos, el responsable del tratamiento debe informar al interesado de la ampliación y de los motivos de esta ([31]). La Data (Use and Access) Act también introdujo un mecanismo que permite a los responsables del tratamiento suspender el plazo para responder a una solicitud en los casos en que sea necesario que el interesado aporte información adicional para detectar los datos solicitados ([32]).

(29) En tercer lugar, en lo que respecta únicamente al derecho de acceso a la información y los datos personales, la Data (Use and Access) Act modifica la sección 45 de la DPA de 2018 para incorporar la aclaración desarrollada en la jurisprudencia nacional vigente —basándose en el principio de proporcionalidad del Derecho de la Unión—, al aclarar que los responsables del tratamiento únicamente deben llevar a cabo búsquedas razonables y proporcionadas de la información y los datos personales solicitados ([33]). Se espera que la nueva disposición se interprete en consonancia con la jurisprudencia existente, que establece que «[…] lo que se pondera en el ejercicio de proporcionalidad es el objeto final de la búsqueda, a saber, el beneficio potencial que el suministro de la información podría aportar al interesado, en comparación con los medios por los que se obtiene dicha información. Se planteará la cuestión de evaluar en cada caso concreto si se realizará un esfuerzo desproporcionado para encontrar y facilitar la información en relación con los beneficios que podría aportar al interesado» ([34]).

(30) Por consiguiente, si bien las modalidades para responder a las solicitudes de los interesados están sujetas a unas normas más exhaustivas, el sistema del Reino Unido sigue garantizando que las solicitudes de los interesados se tramiten en unos plazos razonables determinados sobre la base de unos factores objetivos. Además, las obligaciones sustantivas del responsable del tratamiento al responder a las solicitudes de acceso se enmarcan en la base de las normas jurídicas establecidas que también toman en consideración los intereses del interesado. Por último, ya se establece en las actuales orientaciones de la ICO que un responsable del tratamiento no está obligado a realizar búsquedas que sean irrazonables o desproporcionadas con respecto a la importancia de proporcionar acceso a la información ([35]).

(31) Además, la Data (Use and Access) Act introdujo una nueva sección 45A en la DPA de 2018 en virtud de la cual se establece una exención explícita de la obligación de dar acceso o información a un interesado cuando la información esté protegida por la prerrogativa de confidencialidad ([36]). Esta exención se aplica específicamente a las obligaciones establecidas en la sección 44, apartado 2, y la sección 45, apartado 1, de la DPA de 2018, que obligan a los responsables del tratamiento a informar a las personas del tratamiento de sus datos personales y a garantizarles el acceso a estos ([37]). Aclara que los responsables del tratamiento no están obligados a revelar información si ello supone una violación del secreto profesional. Existe una exención similar en virtud del RGPD del Reino Unido ([38]).

(32) En términos de garantías, cuando se acojan a esta exención, los responsables del tratamiento deben informar por escrito al interesado sin dilación indebida de que se ha aplicado dicha exención, explicar los motivos e informarle de su derecho a solicitar una revisión por parte de la Information Commission o emprender acciones legales ([39]). Para garantizar la rendición de cuentas, la sección 45A, apartado 4, de la DPA de 2018 obliga a los responsables del tratamiento a dejar constancia de la motivación de su decisión de aplicar la exención y a poner dicho documento a disposición de la Information Commission previa solicitud ([40]).

([31]) Sección 54, apartado 3A, y sección 54, apartado 3, letra b), de la DPA de 2018, introducido por la sección 76, apartado 6, de la Data (Use and Access) Act.

([32]) Sección 54, apartados 3C y 3D, de la DPA de 2018, introducidos por la sección 76, apartados 5 y 6, de la Data (Use and Access) Act.

([33]) Sección 45, apartado 2A, de la DPA de 2018, introducido por la sección 78 de la Data (Use and Access) Act.

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

([35]) Puede consultarse en el enlace siguiente (documento en inglés): 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]) Sección 45A, tal como la introdujo la sección 79 de la Data (Use and Access) Act. En el Reino Unido, la prerrogativa de confidencialidad es un derecho legal fundamental que protege determinadas comunicaciones de carácter confidencial entre un cliente y su asesor jurídico de su divulgación sin el consentimiento del cliente. Incluye dos categorías principales: la prerrogativa de asesoramiento jurídico, que protege los intercambios realizados a efectos de obtener o brindar asesoramiento jurídico, y la prerrogativa procesal, que es aplicable a las comunicaciones realizadas para la preparación de un proceso judicial o durante este.

([37]) Las autoridades competentes en virtud de la parte 3 se basaron anteriormente en otras exenciones disponibles en la sección 44, apartado 4 (Derecho a ser informado) y la sección 45, apartado 4 (Derecho de acceso) de la DPA de 2018.

([38]) Anexo 2, apartado 19, de la DPA de 2018.

([39]) Sección 45A, apartado 2, de la DPA de 2018, introducida por la sección 79 de la Data (Use and Access) Act. Cabe aplicar una excepción a esta obligación de notificación cuando la propia transmisión de dicha notificación comprometa el carácter restringido o confidencial de la información. En tales casos, el responsable del tratamiento no tiene la obligación de revelar que se ha aplicado dicha exención ni de proporcionar ninguna explicación adicional.

([40]) Sección 45A de la DPA de 2018, introducida por la sección 79 de la Data (Use and Access) Act.

(33) Por último, la Data (Use and Access) Act ha modificado y consolidado las exenciones existentes en la parte 3 de la DPA de 2018 a disposición de las autoridades competentes con fines de seguridad nacional. La exención relativa a la seguridad nacional permite a las autoridades competentes no aplicar determinadas disposiciones de dicha parte si es necesaria una exención de dicha disposición a efectos de salvaguardar la seguridad nacional ([41]). Refleja las exenciones de seguridad nacional previstas para el tratamiento de datos personales en virtud del RGPD del Reino Unido (previstas en la sección 26 de la DPA de 2018) y en la parte 4 de la DPA de 2018 (prevista en la sección 110 de la DPA de 2018).

(34) La exención de seguridad nacional está sujeta a las mismas limitaciones y garantías que las exenciones en virtud del RGPD del Reino Unido y de la parte 4 de la DPA de 2018, tal como se analiza en los considerandos 64 a 67 y 126 de la Decisión de Ejecución (UE) 2021/1772. En particular, la exención solo podrá aplicarse si es necesario para salvaguardar la seguridad nacional y en la medida en que sea necesario para ello. No se trata de una exención general y el responsable del tratamiento debe considerarla e invocarla caso por caso ([42]). Además, cualquier aplicación de la exención debe cumplir con las normas sobre derechos humanos (amparadas por la Human Rights Act de 1998 y el Convenio Europeo de Derechos Humanos), según las cuales cualquier injerencia en los derechos a la privacidad debe ser necesaria y proporcionada en una sociedad democrática ([43]). Esto también se confirma en las orientaciones de la ICO sobre la aplicación de las exenciones de seguridad nacional ([44]).

2.2.3. *Limitaciones a las transferencias ulteriores*

(35) El nivel de protección de los datos personales que se transfieren desde la Unión Europea a las autoridades encargadas de garantizar el cumplimiento de la ley en el Reino Unido sigue sin verse comprometido por la transferencia ulterior de dichos datos a destinatarios que se encuentran en terceros países. El régimen sobre transferencias internacionales de datos personales desde el Reino Unido sigue siendo muy similar a las normas establecidas en el capítulo V de la Directiva (UE) 2016/680, tal como se evalúa en los considerandos 74 a 87 de la Decisión de Ejecución (UE) 2021/1773.

(36) Si bien la Data (Use and Access) Act modificó el capítulo 5 de la parte 3 de la DPA de 2018 sobre las transferencias de datos personales a las autoridades competentes de terceros países, conserva el requisito esencial en virtud del cual a) la transferencia debe ser necesaria para un fin de aplicación de la ley; b) la transferencia: i) debe basarse en normas de aprobación de la transferencia (mediante las que se sustituyen las anteriores normas en materia de adecuación), ii) debe estar sujeta a unas garantías adecuadas, o iii) debe basarse en circunstancias especiales, y c) el destinatario de la transferencia debe ser: i) una autoridad pertinente (es decir, el equivalente a una autoridad competente) en un tercer país; ii) una organización internacional pertinente, iii) un encargado del tratamiento que actúe por cuenta de una autoridad competente, o iv) una persona que no sea una autoridad pertinente, pero solo en el caso de que la transferencia sea estrictamente necesaria para la consecución de uno de los fines de aplicación de la ley ([45]). Estos principios generales relacionados con las transferencias de datos se reflejan en la sección 73 de la DPA de 2018, que también establece que las transferencias de datos personales a un tercer país o una organización internacional únicamente están permitidas si la transferencia se lleva a cabo en cumplimiento de las demás disposiciones previstas en la parte 3 de la DPA de 2018 ([46]).

(37) Por lo que se refiere específicamente a las normas por las que se aprueba una transferencia, la sección 74AA, apartado 2, de la DPA de 2018 especifica que el secretario de Estado solo puede adoptar dichas normas si considera que se cumple el criterio de protección de datos. Esto significa que la posibilidad de que el Secretario de Estado, introducida en la sección 74AA, apartado 3, de la DPA 2018, tenga en cuenta la conveniencia de facilitar los flujos de datos al elaborar dichas normativas, siempre está sujeta a la condición de que se cumpla la prueba de protección de datos. La nueva sección 74AB ([47]) de la DPA de 2018 formula la norma jurídica del criterio de protección de datos que hay que cumplir, y exige que el nivel de protección de los interesados en los países destinatarios o en organizaciones internacionales no sea significativamente inferior al proporcionado a los interesados en la legislación de protección

([41]) Sección 78A, apartado 1, de la DPA de 2018, introducida por la sección 88 de la Data (Use and Access) Act. De conformidad con la sección 78A, apartados 2 a 4, de la DPA de 2018, la exención permite dejar de aplicar los principios de protección de datos (excepto el principio de legalidad y las condiciones y salvaguardias para el tratamiento de datos sensibles), los derechos individuales, las obligaciones de los responsables y encargados del tratamiento de datos con respecto a las violaciones de la seguridad de los datos, determinadas partes de las normas sobre transferencias internacionales de datos y algunas de las competencias de entrada de la ICO para llevar a cabo inspecciones y adoptar medidas coercitivas.

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

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

([44]) Véase la guía de la ICO sobre la excepción de seguridad y defensa nacional, disponible en el siguiente enlace: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/.

([45]) Sección 73 de la DPA de 2018, en su versión modificada por el apartado 3, párrafos cuarto y quinto, del anexo 8 de la Data (Use and Access) Act.

([46]) Sección 73 de la DPA de 2018, en su versión modificada por el apartado 3, párrafo tercero, del anexo 8 de la Data (Use and Access) Act.

([47]) Introducida mediante el apartado 4, párrafo segundo, del anexo 8, de la Data (Use and Access) Act.

de datos pertinente del Reino Unido. Así, la sección 74AB, apartado 2, de la DPA de 2018 ofrece una lista no exhaustiva de elementos que se han de tener en cuenta a la hora de evaluar si se cumple dicho criterio, como el respeto del Estado de Derecho y de los derechos humanos, la existencia de una autoridad de protección de datos y los poderes de esta, las vías de recurso judicial y extrajudicial, las normas relativas a la transferencia de datos personales desde el país o por la organización internacional a otros países u organizaciones internacionales, las obligaciones internacionales pertinentes del país o la organización, así como la constitución, las tradiciones y la cultura del país o la organización. Si bien reformula la lista de elementos pertinentes recogida en la antigua sección 74A de la DPA de 2018, la nueva disposición conserva los elementos fundamentales de dicha lista y, por tanto, se asemeja a lo establecido en el artículo 36 de la Directiva (UE) 2016/680. Además, las autoridades del Reino Unido han confirmado que el secretario de Estado tendrá en cuenta elementos no enumerados en la sección 74AB, apartado 2, como las leyes y prácticas de un tercer país relativas a la forma en que las autoridades públicas acceden a los datos personales con fines como la seguridad nacional o la aplicación de la ley, en la medida en que afecten al nivel general de protección. Además, las autoridades del Reino Unido consideran que la jurisprudencia pertinente en el tercer país será un componente esencial a la hora de examinar las cuestiones enumeradas de forma no exhaustiva en la sección 74AB, apartado 2, de la DPA de 2018.

(38) Los reglamentos por los que se aprueba una transferencia siguen estando sujetos a los requisitos de procedimiento «generales» previstos en la sección 182 de la DPA de 2018, tal como se establece en el considerando 77 de la Decisión de Ejecución (UE) 2021/1773. En virtud de este procedimiento, el secretario de Estado debe consultar a la ICO al proponer la adopción de normas en materia de adecuación en el Reino Unido ([48]). Una vez que el secretario de Estado ha adoptado las normas, estas se presentan ante el Parlamento y están sujetas al procedimiento de «resolución negativa», en virtud del cual ambas cámaras del Parlamento pueden examinarlas y tienen la capacidad de aprobar una moción que anule las normas en un plazo de cuarenta días ([49]).

(39) Con respecto a las garantías adecuadas, la sección 75 de la DPA de 2018, modificada por el apartado 6 del anexo 8 de la Data (Use and Access) Act, establece que dichas transferencias solo pueden llevarse a cabo si: a) un instrumento jurídico adecuado vincula al destinatario previsto de los datos, es decir, un instrumento que cumpla las condiciones establecidas en el nuevo apartado 4, en particular que cada autoridad competente del Reino Unido que sea parte en el instrumento, actuando de manera razonable y proporcionada, considere que se cumple el criterio de protección de datos, o b) el responsable del tratamiento, actuando de manera razonable y proporcionada, considere que se cumple el criterio de protección de datos en relación con la transferencia o ese tipo de transferencia. La sección 75, apartado 5, de la DPA de 2018 que se ha insertado aclara que el criterio de protección de datos se cumple si, debido a las garantías requeridas, el nivel de protección proporcionado a los interesados no es significativamente inferior después de la transferencia al nivel establecido en la legislación pertinente del Reino Unido en materia de protección de datos. Esto es similar a las medidas establecidas en el artículo 37 de la Directiva (UE) 2016/680. Como consecuencia de ello, se aplican las mismas normas jurídicas en la UE y en el Reino Unido en relación con la aprobación de una transferencia sujeta a las garantías apropiadas. De acuerdo con la nueva sección 75(6) de la DPA de 2018, lo que es razonable y proporcionado debe determinarse por referencia a todas las circunstancias, o a las circunstancias probables, de la transferencia o el tipo de transferencia, también la naturaleza y el volumen de los datos personales transferidos.

(40) En lo que respecta a las transferencias basadas en circunstancias especiales de conformidad con la sección 76 de la DPA de 2018, se introducen varias modificaciones técnicas para aclarar las condiciones en las que pueden realizarse dichas transferencias, pero que no afectan al nivel de protección de los datos personales en el Reino Unido ([50]).

(41) En términos de aplicación de las normas sobre transferencias internacionales del Reino Unido, ha habido algunos cambios desde la adopción de la Decisión de Ejecución (UE) 2021/1773.

(42) En primer lugar, tras la celebración de un memorando de entendimiento en 2022 entre el Ministerio del Interior y la ICO, en el que se definían sus respectivas funciones en la realización de las evaluaciones de adecuación de la aplicación de la ley ([51]), el Reino Unido llevó a cabo evaluaciones de los marcos de protección de datos en la Bailía de

([48]) Véase el memorando de entendimiento entre el secretario de Estado del Departamento de Cultura, Medios de Comunicación y Deporte y la Oficina del Comisionado de Información sobre la función de la ICO en relación con la nueva evaluación de adecuación del Reino Unido, disponible en el siguiente enlace: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([49]) Si se aprueba dicha votación, la norma dejará en última instancia de tener efecto jurídico.

([50]) Anexo 8, apartado 7, de la Data (Use and Access) Act.

([51]) Puede consultarse en el enlace siguiente (documento en inglés): https://ico.org.uk/media2/about-the-ico/mou/4025752/ico-ho-mou.pdf.

Guernesey, la Bailía de Jersey y la Isla de Man. Como resultado de ello, el Reino Unido adoptó normas en materia de adecuación para Guernesey en julio de 2023 ([52]), para Jersey en noviembre de 2023 ([53]) y para la Isla de Man en enero de 2025 ([54]). Dichas normas confirman que cada jurisdicción garantiza un nivel de protección adecuado para los datos personales transferidos en virtud de la parte 3 de la DPA de 2018. Aunque estas normas se adoptaron inicialmente con arreglo al marco jurídico anterior, la evaluación que los sustenta sigue siendo válida con arreglo al marco actualizado. Como consecuencia de ello, las normas siguen facilitando la cooperación internacional en el ámbito de la aplicación de la ley.

(43) La Comisión también evaluó los marcos de protección de datos para el tratamiento de datos personales en el contexto de la aplicación del Derecho penal, así como las normas sobre el acceso a los datos personales por parte de las autoridades públicas con fines de seguridad nacional en las Bailía de Jersey y Guernesey y la Isla de Man, al evaluar el funcionamiento de las decisiones de adecuación adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE de conformidad con el artículo 97 del Reglamento (UE) 2016/679. Sobre la base, entre otras cosas, de esta evaluación, la Comisión llegó a la conclusión de que los tres países y territorios siguen proporcionando un nivel adecuado de datos personales transferidos desde la UE ([55]).

(44) En segundo lugar, en 2022, el Reino Unido y los Estados Unidos celebraron el Acuerdo entre el Reino Unido y los Estados Unidos en materia de Protección de Datos y Privacidad ([56]), que aplica los términos del Acuerdo Marco entre la UE y los Estados Unidos ([57]) *mutatis mutandis*, garantizando una protección equivalente en el contexto de los intercambios de datos entre el Reino Unido y los Estados Unidos a efectos de aplicación de la ley.

(45) En tercer lugar, en 2023 y 2025 la ICO actualizó sus directrices sobre transferencias internacionales con arreglo a la parte 3, capítulo 5, de la DPA de 2018 ([58]). En la actualización de 2023 se aclaró el significado del requisito de que las transferencias de datos sean «estrictamente necesarias» cuando los destinatarios no sean las autoridades pertinentes encargadas de garantizar el cumplimiento de la ley, brindando de este modo mayor seguridad a los responsables del tratamiento de los datos a la hora de evaluar la legalidad de dichas transferencias. En 2025, la lista de países y territorios adecuados se actualizó a raíz de las normas de adecuación del Reino Unido para la Isla de Man.

2.2.4. *Mecanismo de decisión automatizado*

(46) Si bien conserva varios elementos de las normas relativas a las decisiones automatizadas evaluadas en los considerandos 72 y 73 de la Decisión de Ejecución (UE) 2021/1773, la Data (Use and Access) Act ha modificado algunos aspectos de dichas normas.

(47) En primer lugar, la nueva sección 50B de la DPA de 2018 establece una prohibición general de tomar decisiones importantes basadas total o parcialmente en el tratamiento de categorías especiales de datos personales. No obstante, contempla dos excepciones a esta prohibición: que el interesado haya dado su consentimiento expreso para dicho tratamiento o que sea una decisión requerida o autorizada por la ley ([59]).

(48) En segundo lugar, la nueva sección 50C de la DPA de 2018 obliga a que los responsables del tratamiento apliquen garantías con respecto a toda decisión significativa basada total o parcialmente en datos personales y basada únicamente en el tratamiento automatizado. Dichas garantías deben incluir la facilitación de información relativa al

([52]) Puede consultarse en el enlace siguiente (documento en inglés): https://www.legislation.gov.uk/uksi/2023/1221/contents/made.
([53]) Puede consultarse en el enlace siguiente (documento en inglés): https://www.legislation.gov.uk/uksi/2023/744/made.
([54]) Puede consultarse en el enlace siguiente (documento en inglés): https://www.legislation.gov.uk/uksi/2025/89/contents/made.
([55]) Informe de la Comisión al Parlamento Europeo y al Consejo, de 15 de enero de 2024, sobre la primera revisión del funcionamiento de las decisiones de adecuación adoptadas con arreglo al artículo 25, apartado 6, de la Directiva 95/46/CE, que se puede consultarse en el enlace siguiente: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52024DC0007; y los informes por país sobre el funcionamiento de las decisiones de adecuación adoptadas en virtud de la Directiva 95/46/CE que acompañan al documento Informe de la Comisión al Parlamento Europeo y al Consejo sobre la primera revisión del funcionamiento de las decisiones de adecuación adoptadas con arreglo al artículo 25, apartado 6, de la Directiva 95/46/CE, disponibles en el siguiente enlace: https://commission.europa.eu/document/download/f8229eb2-1a36-4cf5-a099-1cd001664bff_en?filename=JUST_template_comingsoon_Commission%20Staff%20Working%20Document%20-%20Report%20on%20the%20first%20review%20of%20the%20functioning.pdf.
([56]) Puede consultarse en el enlace siguiente (documento en inglés): 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-offe.
([57]) Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la protección de datos personales relativa a la prevención, investigación, detección o enjuiciamiento de infracciones penales (DO L 336 de 10.12.2016, p. 3), que puede consultarse en el enlace siguiente: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:22016A1210(01)&from=ES.
([58]) Puede consultarse en el enlace siguiente (documento en inglés): https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/international-transfers/.
([59]) Sección 50B de la DPA de 2018, introducida por la sección 80, apartado 3, de la Data (Use and Access) Act.

proceso de toma de decisiones al interesado, permitiendo que este último impugne la decisión o presente observaciones, y asegurar que el interesado pueda solicitar intervención humana en el proceso de toma de decisiones ([60]). Si bien la sección 50C, apartado 4, de la DPA de 2018 establece una exención de la aplicación de estas garantías si dicha exención es necesaria para evitar obstaculizar una investigación, indagación o procedimiento oficial o legal, para evitar perjudicar la prevención, detección, investigación o enjuiciamiento de delitos penales o la ejecución de sanciones penales, para proteger la seguridad pública, o para salvaguardar la seguridad nacional o proteger los derechos y libertades de otras personas, la aplicación de estas salvaguardias solo se suspende temporalmente, dado que el responsable del tratamiento está obligado a reconsiderar la decisión tan pronto como sea razonablemente posible y que existe una participación humana significativa en la reconsideración de la decisión ([61]).

(49) Además, la nueva sección 50A de la DPA de 2018 aclara la definición de una decisión «basada únicamente en el tratamiento automatizado» al disponer que dicha decisión se caracteriza por la ausencia de una intervención humana significativa en el proceso decisorio. Es importante señalar que los responsables del tratamiento tienen la obligación de evaluar en qué medida la elaboración de perfiles contribuye a una decisión para determinar si la intervención humana ha sido significativa. La sección 50A de la DPA de 2018 también aclara que una «decisión significativa» es aquella que produce efectos jurídicos en el interesado o le perjudica significativamente ([62]). Esta limitación a las decisiones que tienen un efecto adverso para el interesado refleja el hecho de que, a diferencia del tratamiento con arreglo al RGPD del Reino Unido, es poco probable que las autoridades competentes adopten decisiones que los interesados consideren positivas.

(50) Por último, la nueva sección 50D de la DPA de 2018 otorga al secretario de Estado la facultad de adoptar legislación derivada para describir qué constituye y qué no constituye una participación humana significativa, qué decisiones se consideran y cuáles no se consideran que tienen un efecto adverso igualmente significativo sobre los interesados. También permite al secretario de Estado elaborar legislación derivada para i) añadir nuevas salvaguardias; ii) imponer requisitos que complementen las garantías existentes; y iii) definir medidas que no cumplan las garantías ([63]). Es importante señalar que, antes de adoptar reglamentos de conformidad con la sección 50D de la DPA de 2018., el secretario de Estado debe consultar a la ICO ([64]), y los reglamentos están sujetos al procedimiento de resolución afirmativa ([65]), lo que significa que deben ser aprobados por ambas cámaras del Parlamento del Reino Unido antes de que puedan promulgarse.

(51) Si bien la Data (Use and Access) Act ha modificado así el marco aplicable a las decisiones automatizadas, conviene señalar que en el marco jurídico del Reino Unido las decisiones automatizadas siguen estando sujetas a una serie de garantías clave que exigen el derecho a obtener intervención humana en todos los casos de toma de decisiones automatizadas, es decir, sobre la base del tratamiento de datos personales sensibles y no sensibles ([66]).

2.2.5. *Rendición de cuentas*

(52) El ordenamiento jurídico del Reino Unido sigue respetando el principio de rendición de cuentas consagrado en la Directiva (UE) 2016/680, que exige a las autoridades públicas que adopten las oportunas medidas de carácter técnico y organizativo con el fin de garantizar y demostrar el cumplimiento de las obligaciones que les correspondan en materia de protección de datos, tal como se evalúa en los considerandos 88 a 92 de la Decisión de Ejecución (UE) 2021/1773.

(53) La obligación de que las autoridades competentes mantengan registros de sus actividades de tratamiento, como la recogida, modificación, consulta, comunicación, combinación y supresión de datos personales ([67]) representa una de las medidas contempladas en la DPA de 2018 para garantizar la rendición de cuentas y permitir que los responsables y los encargados del tratamiento demuestren el cumplimiento. La Data (Use and Access) Act modifica las obligaciones específicas aplicables a los responsables del tratamiento conforme a lo establecido en dicha disposición al solo eliminar de la sección 62 de la DPA de 2018 el requisito de que los responsables del tratamiento registren una justificación cada vez que se consulten o comuniquen datos personales ([68]). Es importante señalar que el requisito que obliga a los responsables del tratamiento a registrar las actividades de tratamiento sigue en vigor con el fin de conservar el principal mecanismo para garantizar la rendición de cuentas.

([60]) Sección 50C de la DPA de 2018, introducida por la sección 80, apartado 3, de la Data (Use and Access) Act.
([61]) Sección 50C, apartados 3 y 4, de la DPA de 2018, introducidos por la sección 80, apartado 3, de la Data (Use and Access) Act.
([62]) Sección 50A de la DPA de 2018, introducida por la sección 80, apartado 3, de la Data (Use and Access) Act.
([63]) Artículo 50D de la DPA de 2018, introducido por la sección 80, apartado 3, de la Data (Use and Access) Act. Toda normativa elaborada en virtud de estas facultades está sujeta al procedimiento de resolución afirmativa, lo que garantiza la supervisión del Parlamento. Esta normativa no puede modificar los requisitos establecidos en la sección 50C.
([64]) Artículo 182, apartado 2, de la DPA de 2018.
([65]) Sección 50D, apartado 5, de la DPA de 2018.
([66]) Sección 50C, apartado 2, letra c), de la DPA de 2018.
([67]) Artículo 62 de la DPA de 2018. Véase también el considerando 90 de la Decisión de Ejecución (UE) 2021/1773.
([68]) Sección 82 de la Data (Use and Access) Act.

2.3. **Supervisión y cumplimiento de las normas**

2.3.1. *Supervisión independiente*

(54) En el Reino Unido, de la supervisión y el cumplimiento de las normas del marco de protección de datos se sigue encargando una autoridad de control en materia de protección de datos independiente, como se analiza en los considerandos 93 a 99 de la Decisión de Ejecución (UE) 2021/1773. La Data (Use and Access) Act modifica la estructura de gobernanza de esta autoridad al constituir una persona jurídica, la Information Commission [Comisión de Información], que reemplazará a la ICO, que se había estructurado como una persona jurídica unipersonal.

(55) Más concretamente, las medidas de gobernanza establecidas en la Data (Use and Access) Act, una vez aplicadas, suprimirán la ICO y transferirán las funciones, el personal y los bienes de la ICO al nuevo organismo, la Information Commission. La Information Commission está compuesta por miembros ejecutivos y no ejecutivos ([69]). La Ley también establece disposiciones para que el Information Commissioner pase a desempeñar la función de presidente de la Information Commission, que es uno de los miembros no ejecutivos ([70]). La Data (Use and Access) Act dispone además que en la medida en que resulte apropiado como consecuencia de la transferencia de funciones, las referencias al Information Commissioner en todos los actos legislativos u otros documentos (tanto durante su aprobación como durante su elaboración) deben tratarse como referencias a la Information Commission. Para desempeñar sus funciones, esta podrá crear comités y delegar funciones en un miembro, un empleado o un comité ([71]), y podrá adoptar disposiciones para regular su procedimiento y el procedimiento de los comités, también en lo que se refiere al *quorum* y a la adopción de decisiones por mayoría. Estos procedimientos deben hacerse públicos ([72]).

(56) Es importante señalar que la independencia de la Information Commission está sujeta a las mismas garantías, también respecto de las normas sobre el nombramiento y la destitución de su presidente, que las evaluadas en los considerandos 95 a 98 de la Decisión de Ejecución (UE) 2021/1773 ([73]). Se aplican protecciones similares a los demás miembros no ejecutivos de la Information Commission. En particular, su presidente es nombrado por Su Majestad sobre la base de una recomendación del secretario de Estado. Se selecciona en atención a sus méritos y sobre la base de un concurso justo y abierto ([74]). Los demás miembros no ejecutivos son nombrados por el secretario de Estado, previa consulta al presidente. Los candidatos solo pueden ser recomendados para su nombramiento o nombrados si son seleccionados sobre la base de sus méritos con arreglo a un concurso justo y abierto, y si el secretario de Estado está convencido de que no tienen un conflicto de intereses ([75]). Los miembros ejecutivos son empleados de la Information Commission contratados según los términos y condiciones determinados por los miembros no ejecutivos ([76]). El director ejecutivo es nombrado por el presidente y otros miembros no ejecutivos, tras consultar con el secretario de Estado. Los nombramientos de los miembros ejecutivos también están sujetos a una selección por méritos sobre la base de un concurso justo y abierto ([77]).

(57) El presidente solamente puede ser destituido de su cargo por Su Majestad en respuesta a un discurso de ambas cámaras del Parlamento y únicamente si el secretario de Estado ha presentado un informe ante dichas cámaras en el que manifieste su convencimiento de que el presidente es culpable de una falta grave, tiene un conflicto de intereses, no cumple los requisitos de información específicos respecto de los posibles conflictos de intereses o bien está incapacitado o no es apto para desempeñar las funciones del presidente, o no desea hacerlo ([78]). El secretario de Estado solo podrá destituir a los miembros no ejecutivos si considera que se cumplen las condiciones específicas establecidas en la legislación. Entre ellas se incluyen los conflictos de intereses, las faltas graves o la incapacidad, falta de voluntad o incapacidad para desempeñar sus funciones. En cuanto a las garantías adicionales, el secretario de Estado está obligado a hacer pública la decisión de hacerlo y a proporcionar al miembro una exposición de los motivos de la expulsión ([79]).

([69]) Anexo 12A, apartado 3, párrafo primero, de la DPA de 2018.
([70]) Secciones 117, 118, 119 y 120 junto con el anexo 14 de la Data (Use and Access) Act.
([71]) Anexo 12A, apartados 13 y 14, de la DPA de 2018.
([72]) Anexo 12A, apartado 16, de la DPA de 2018.
([73]) Artículo 52 del RGPD del Reino Unido y anexo 12A de la DPA de 2018, introducido por la sección 117 del Data (Use and Access) Act.
([74]) Anexo 12A, apartado 5, párrafo primero, de la DPA de 2018.
([75]) Anexo 12A, apartado 3, párrafo segundo, y apartados 5 y 6, de la DPA de 2018.
([76]) Anexo 12A, apartado 11, de la DPA de 2018.
([77]) Anexo 12A, apartado 5, párrafo segundo, de la DPA de 2018.
([78]) Anexo 12A, apartado 7, párrafos sexto y séptimo, de la DPA de 2018.
([79]) Anexo 12A, apartado 9, párrafos sexto, séptimo, octavo y noveno, de la DPA de 2018.

(58) La Data (Use and Access) Act no altera las responsabilidades principales de la Information Commission, que seguirá desempeñando las funciones establecidas en el anexo 13 de la DPA de 2018, como, por ejemplo, controlar y garantizar el cumplimiento de la parte 3 de la DPA de 2018, asesorar al Parlamento y al Gobierno, promover la sensibilización del público, apoyar a los responsables y encargados del tratamiento de los datos en el cumplimiento de sus obligaciones, e informar a las personas de sus derechos ([80]). La Data (Use and Access) Act aclara que, en el ejercicio del deber de garantizar un nivel de protección adecuado de los datos personales, la Information Commission debe tener en cuenta los intereses de los interesados, los responsables del tratamiento y otras partes, considerar el interés público más amplio y promover la confianza del público en el tratamiento de los datos personales. ([81]).

(59) Además, la Data (Use and Access) Act especifica que la Information Commission deberá tener en cuenta, en la medida en que sea pertinente en cada caso, la promoción de la innovación y la competencia, la importancia de la prevención, investigación, detección y enjuiciamiento de delitos penales, la necesidad de salvaguardar la seguridad pública y la seguridad nacional, y las necesidades específicas relacionadas con la protección de los menores al desempeñar sus funciones en virtud de la legislación sobre protección de datos ([82]). La legislación de la UE en materia de protección de datos también reconoce la necesidad de equilibrar la protección de los datos personales con otros derechos y objetivos fundamentales, como la seguridad y la justicia ([83]).

2.3.2. *Ejecución, en particular las sanciones, y acciones administrativas y judiciales*

(60) Las competencias y funciones de la Information Commission siguen siendo equivalentes a las de las autoridades de control en materia de protección de datos de los Estados miembros en virtud de los artículos pertinentes de la Directiva (UE) 2016/680 ([84]), como se analiza en los considerandos 100 a 109 de la Decisión de Ejecución (UE) 2021/1773.

(61) La Data (Use and Access) Act ha introducido una serie de aclaraciones específicas relacionadas con el ejercicio de algunas de dichas competencias.

(62) La sección 97 de la Data (Use and Access) Act modifica la sección 142 de la DPA de 2018 con el fin de permitir expresamente que la Information Commission requiera no solo información sino también documentos específicos, mejorando así su capacidad para investigar y verificar el cumplimiento.

(63) La sección 98 de la Data (Use and Access) Act refuerza las competencias de la Information Commission en virtud de la sección 146 de la DPA de 2018 al permitir que la Information Commission solicite a un responsable o encargado del tratamiento de los datos que encargue un informe independiente sobre un asunto concreto. Dicho informe debe ser elaborado por una «persona autorizada» y la Information Commission es la máxima autoridad con respecto a la autorización de la persona designada o la designación de otra persona si no se propone ninguna persona adecuada o si no actúa el responsable del tratamiento ([85]). El aviso de evaluación puede especificar el formato, el contenido y el plazo de presentación del informe ([86]). Todos los costes relacionados, como las tarifas aprobadas de la persona, deben ser asumidos por el responsable o el encargado del tratamiento ([87]).

(64) La sección 100 de la Data (Use and Access) Act establece los avisos de entrevista como un nuevo instrumento de ejecución de conformidad con la sección 148A de la DPA de 2018. La Information Commission puede exigir a una persona que asista a entrevistas con garantías, como la protección contra la autoincriminación y el privilegio legal ([88]).

(65) La sección 101 de la Data (Use and Access) Act modifica el anexo 16 de la DPA de 2018 para otorgar a la Information Commission mayor flexibilidad en relación con la emisión de los avisos de sanción. Aunque la norma general sigue siendo el plazo actual de seis meses para la emisión de un aviso de sanción firme tras un aviso de intención, dicha sección permite a la Information Commission emitir un aviso de sanción después de dicho plazo cuando no sea razonablemente posible cumplir con este último. En tales casos, el aviso debe emitirse tan pronto como sea razonablemente posible. Además, si la Information Commission decide no emitir un aviso de sanción, debe informar a la persona en cuestión por escrito en un plazo de seis meses o tan pronto como sea razonablemente posible a partir de ese momento. Dicha sección también introduce un nuevo requisito en virtud del cual la Information Commission debe publicar orientaciones relativas a las circunstancias en las que puedan requerirse más de seis meses para emitir un aviso de sanción.

([80]) Anexo 13 de la DPA de 2018.
([81]) Sección 91 de la Data (Use and Access) Act, introducida por la sección 120A de la DPA de 2018.
([82]) Sección 91 de la Data (Use and Access) Act, introducida por la sección 120B de la DPA de 2018.
([83]) Véase, en particular, el considerando 2 de la Directiva (UE) 2016/680.
([84]) Anexo 13, apartado 2, de la DPA de 2018.
([85]) Sección 98 de la Data (Use and Access) Act, introducida por la sección 146A de la DPA de 2018.
([86]) Sección 98 de la Data (Use and Access) Act, introducida por la sección 146, apartad 3A, de la DPA de 2018.
([87]) Sección 98 de la Data (Use and Access) Act, introducida por la sección 146, apartad 11A, de la DPA de 2018.
([88]) Sección 98 de la Data (Use and Access) Act, introducida por la sección 146, apartado 8A, de la DPA de 2018.

(66) La sección 102 de la Data (Use and Access) Act introduce nuevas obligaciones de notificación para la Information Commission. Modifica la sección 139 y añade una sección nueva, la 161A, en la DPA de 2018, obligando a la Information Commission a publicar un informe anual sobre la acción reguladora. Dicho informe debe detallar cómo se han ejercido los poderes de investigación y ejecución en virtud del RGPD del Reino Unido y las partes 3 y 4 de la DPA de 2018. También debe dar a conocer el número de avisos de sanción emitidos después del plazo de seis meses tras un aviso de intención y aportar justificaciones del retraso. Además, el informe debe explicar cómo la Information Commission ha seguido sus propias directrices a la hora de adoptar decisiones reguladoras.

(67) La sección 103 de la Data (Use and Access) Act refuerza el procedimiento de reclamación disponible para los interesados. Agrega nuevas secciones, la 164A y la 164B, a la DPA de 2018. La sección 164A establece que los interesados tienen derecho a presentar reclamaciones directamente ante los responsables del tratamiento si creen que se han vulnerado sus derechos en virtud del RGPD del Reino Unido o la parte 3 de la DPA de 2018. Los responsables del tratamiento deben facilitar este proceso, admitir las reclamaciones en un plazo de treinta días y responder sin demora indebida. También deben mantener a los reclamantes informados de los avances y los resultados. La sección 164B otorga al secretario de Estado la facultad de formular normativa que obligue a los responsables del tratamiento a informar del número de reclamaciones recibidas.

(68) La sección 104 de la Data (Use and Access) Act introduce la sección 180A en la DPA de 2018 para aclarar cuáles son las competencias de los tribunales en relación con procedimientos relativos a las solicitudes de acceso de los interesados. De acuerdo con esta disposición, los tribunales pueden exigir a los responsables del tratamiento que aporten la información en cuestión para su inspección por el tribunal a la hora de decidir si un sujeto tiene derecho a ella. Sin embargo, la información no puede comunicarse al interesado a menos que el tribunal determine que tiene derecho a acceder a ella. Esta sección aclara que los tribunales puedan examinar el material en disputa sin comunicárselo prematuramente al reclamante, con lo que se restaura una garantía que existía previamente en virtud de la Data Protection Act de 1998.

(69) En cuanto al ejercicio de estas competencias, desde la adopción de la Decisión de Ejecución (UE) 2021/1773, el Information Commissioner ha tramitado numerosas reclamaciones ([89]) y ha llevado a cabo varias investigaciones y adoptado medidas de ejecución con respecto al tratamiento de datos por parte de las autoridades encargadas de garantizar el cumplimiento de la ley. Entre 2021 y 2025, el Information Commissioner llevó a cabo investigaciones y emitió amonestaciones contra varios órganos policiales por distintos incumplimientos de sus obligaciones en materia de protección de datos, por ejemplo, en la respuesta a solicitudes de acceso a los datos, en el establecimiento de medidas de seguridad relacionadas con datos de videovigilancia, en el tratamiento de antecedentes penales sensibles, al fusionar los datos de distintas personas, o al comunicar datos personales a terceros ([90]). El Information Commissioner también emitió y actualizó directrices, dictámenes y documentos de orientación, por ejemplo, sobre el derecho de acceso o sobre cómo tramitar solicitudes manifiestamente infundadas o excesivas con arreglo a la parte 3 de la DPA de 2018 ([91]), o actualizó directrices existentes, como su *Guide to Law Enforcement Processing* [«Guía para el tratamiento con fines de aplicación de la ley», documento en inglés] ([92]).

3. **CONCLUSIÓN**

(70) La Comisión considera que la parte 3 de la DPA de 2018, sigue garantizando un nivel de protección de los datos personales transferidos con fines penales desde las autoridades competentes de la Unión Europea a las autoridades competentes del Reino Unido que es esencialmente equivalente al que garantiza la Directiva (UE) 2016/680.

([89]) Por ejemplo, la Information Commission recibió en 2023-2024 1 890 reclamaciones sobre la base del RGPD o la DPA de 2018 relacionadas con organizaciones pertenecientes a los subsectores «autoridad policial», «fuerzas policiales» y «comisarios de policía». Véase también el *Annual Report and Financial Statements 2023-24* [«Informe anual y estados financieros 2023-2024», documento en inglés] del Information Commissioner, disponible en el siguiente enlace: https://ico.org.uk/media2/migrated/4030348/annual-report-2023-24.pdf.

([90]) Puede encontrarse información complementaria en el enlace siguiente (documento en inglés): https://ico.org.uk/action-weve-taken/enforcement/?ensector=criminal-justice.

([91]) Puede consultarse en el enlace siguiente (documento en inglés): https://ico.org.uk/for-organisations/law-enforcement/the-right-of-access-part-3-of-the-dpa-2018/ y https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/individual-rights/manifestly-unfounded-and-excessive-requests/.

([92]) Puede consultarse en el enlace siguiente (documento en inglés): https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/.

(71) Además, la Comisión considera que, en su conjunto, los mecanismos de supervisión y las vías de impugnación contemplados en el Derecho del Reino Unido siguen siendo suficientes para detectar y sancionar en la práctica las vulneraciones de la normativa de protección de datos y brindan al interesado medios jurídicos para solicitar el acceso a sus datos personales y, en su caso, su rectificación o supresión.

(72) Por lo tanto, debe concluirse que el Reino Unido sigue garantizando un nivel adecuado de protección a efectos del artículo 36, apartado 2, de la Directiva (UE) 2016/680, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea.

4. EFECTOS DE LA PRESENTE DECISIÓN Y ACTUACIÓN DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS

(73) Los Estados miembros y sus organismos están obligados a adoptar las medidas necesarias para dar cumplimiento a los actos de las instituciones de la Unión, ya que estos disfrutan de una presunción de legalidad y producen, por consiguiente, efectos jurídicos en tanto no hayan perdido vigencia o sido revocados, anulados en el marco de un recurso de anulación o declarados inválidos a raíz de una cuestión prejudicial o de una excepción de ilegalidad.

(74) Por lo tanto, toda decisión de adecuación de la Comisión adoptada en virtud del artículo 36, apartado 3, de la Directiva (UE) 2016/680 vincula a todos los organismos de los Estados miembros destinatarios, incluidas sus autoridades de control independientes. En particular, durante el período de aplicación de la Decisión de Ejecución (UE) 2021/1773, modificada por la presente Decisión, pueden producirse transferencias de un responsable o encargado del tratamiento en la Unión a responsables o encargados del tratamiento en el Reino Unido sin necesidad de obtener ninguna autorización adicional.

(75) Al mismo tiempo, cabe recordar que, de conformidad con el artículo 47, apartado 5, de la Directiva (UE) 2016/680 y como explicó el Tribunal de Justicia en la sentencia *Schrems I*, cuando una autoridad nacional de protección de datos cuestiona, en especial a raíz de una reclamación, la compatibilidad de una decisión de adecuación de la Comisión con los derechos fundamentales de la persona a la privacidad y la protección de los datos, el Derecho nacional debe proporcionarle un recurso legal para presentar esas objeciones ante un tribunal nacional, al que podrá exigirse la presentación de una petición de decisión prejudicial al Tribunal de Justicia ([93]).

5. SEGUIMIENTO

(76) De conformidad con el artículo 36, apartado 4, de la Directiva (UE) 2016/680, la Comisión supervisará de manera continuada los acontecimientos pertinentes en el Reino Unido a fin de valorar si esta aún garantiza un nivel de protección esencialmente equivalente. Esta supervisión es especialmente importante porque el Reino Unido aplicará y hará cumplir un régimen modificado de protección de datos. Asimismo, el marco modificado de protección de datos del Reino Unido otorga al secretario de Estado la facultad de especificar en mayor medida este marco a través del Derecho derivado. A este respecto, debe prestarse especial atención a dichas especificaciones adicionales, así como a la aplicación en la práctica de las normas modificadas del Reino Unido sobre transferencias de datos personales a terceros países; a la eficacia del ejercicio de los derechos individuales, incluida cualquier evolución pertinente de la legislación y la práctica en relación con las excepciones o restricciones de dichos derechos recientemente introducidas, al funcionamiento de la ICO reestructurada, también con respecto a la tramitación de reclamaciones y la aplicación de poderes correctivos. La supervisión de la Comisión se debe basar en, entre otros elementos, los avances de la jurisprudencia y la supervisión de la ICO y otros organismos independientes.

(77) Con el fin de facilitar esta supervisión, las autoridades del Reino Unido deben informar regular y puntualmente a la Comisión de cualquier cambio sustancial en el ordenamiento jurídico del Reino Unido que tenga un impacto en el marco jurídico objeto de la Decisión de Ejecución (UE) 2021/1773, modificada por la presente Decisión, así como de cualquier evolución en las prácticas relacionadas con el tratamiento de los datos personales evaluados en la Decisión de Ejecución (UE) 2021/1773, modificada por la presente Decisión, en particular en lo que respecta a los elementos señalados en el considerando 39.

(78) Además, a fin de que la Comisión pueda desempeñar eficazmente su función de supervisión, los Estados miembros deben informarle de cualquier medida pertinente adoptada por las autoridades nacionales de protección de datos, en particular en lo que respecta a las consultas o las reclamaciones de los interesados de la Unión en relación con la transferencia de datos personales desde la UE a las autoridades competentes del Reino Unido. También debe informarse a la Comisión de todo indicio de que las acciones de las autoridades públicas del Reino Unido responsables de la prevención, investigación, detección o enjuiciamiento de infracciones penales, incluidos los órganos de supervisión, no garantizan el nivel de protección necesario.

([93]) *Schrems I*, apartado 65.

(79) Cuando la información disponible, en particular la información resultante de la supervisión de la presente Decisión o proporcionada por las autoridades del Reino Unido o de los Estados miembros, revele que el nivel de protección ofrecido por el Reino Unido podría ya no ser adecuado, la Comisión debe informar sin demora a las autoridades competentes del Reino Unido y solicitar que se adopten medidas adecuadas dentro de un plazo determinado, el cual no podrá exceder de tres meses. En caso necesario, este plazo podrá ampliarse por un período determinado, teniendo en cuenta la naturaleza del asunto en cuestión o las medidas que deban tomarse.

(80) Si, al expirar dicho plazo determinado, las autoridades competentes del Reino Unido no han adoptado dichas medidas o no han demostrado satisfactoriamente de otro modo que la presente Decisión sigue basándose en un nivel de protección adecuado, la Comisión iniciará el procedimiento a que se refiere el artículo 58, apartado 2, de la Directiva (UE) 2016/680 con el fin de suspender o derogar, total o parcialmente, esta Decisión.

(81) La Comisión también puede iniciar este procedimiento para modificar la Decisión de Ejecución (UE) 2021/1773, modificada por la presente Decisión., en particular con el fin de imponer condiciones adicionales a las transferencias de datos o con el fin de limitar la conclusión de adecuación solo a las transferencias de datos para las que se siga garantizando un nivel de protección adecuado.

(82) Por razones imperiosas de urgencia debidamente justificadas, la Comisión debe hacer uso de la competencia de adoptar, de conformidad con el procedimiento a que se refiere el artículo 58, apartado 3, de la Directiva (UE) 2016/680, actos de ejecución inmediatamente aplicables que suspendan, deroguen o modifiquen la presente Decisión.

6. REVISIÓN, DURACIÓN Y RENOVACIÓN DE LA PRESENTE DECISIÓN

(83) En aplicación del artículo 36, apartado 3, de la Directiva (UE) 2016/680 y teniendo en cuenta el hecho de que el nivel de protección que ofrece el ordenamiento jurídico del Reino Unido puede ser objeto de modificación, la Comisión, tras la adopción de la presente Decisión, debe revisar periódicamente si las conclusiones relativas a la adecuación del nivel de protección garantizado por el Reino Unido siguen estando justificadas de hecho y de Derecho. Estas evaluaciones deben tener lugar al menos cada cuatro años y deben abarcar todos los aspectos del funcionamiento de la presente Decisión, en particular el funcionamiento de los mecanismos de supervisión y ejecución pertinentes.

(84) Para llevar a cabo la revisión, la Comisión debe reunirse con los representantes pertinentes de las autoridades del Reino Unido, incluida la Information Commission. La participación en esta reunión debe estar abierta a los representantes de los miembros del Comité Europeo de Protección de Datos. En el marco de la revisión, la Comisión debe solicitar al Reino Unido que facilite información completa sobre todos los aspectos pertinentes a efectos de la conclusión de adecuación. La Comisión también debe pedir explicaciones sobre cualquier información pertinente para la presente Decisión que haya recibido, en particular del Comité Europeo de Protección de Datos, de las distintas autoridades de protección de datos y de los grupos de la sociedad civil y los informes públicos o las noticias los medios de comunicación o cualquier otra fuente de información disponible.

(85) Sobre la base de la revisión, la Comisión debe elaborar un informe público que presentará al Parlamento Europeo y al Consejo.

(86) La Comisión también debe tener en cuenta que el marco de protección de datos evaluado en la presente Decisión y en la Decisión de Ejecución (UE) 2021/1773 puede seguir evolucionando.

(87) Por tanto, conviene estipular que la presente Decisión se aplicará durante un período de seis años a partir de su entrada en vigor.

(88) Cuando, en particular, la información resultante de la supervisión de la presente Decisión revele que las conclusiones relativas a la adecuación del nivel de protección garantizado en el Reino Unido siguen estando justificadas de hecho y de derecho, la Comisión debe, a más tardar seis meses antes de que la presente Decisión deje de aplicarse, iniciar el procedimiento para modificar la presente Decisión ampliando su ámbito temporal de aplicación, en principio, por un período adicional de cuatro años. Cualquier acto de ejecución que modifique la presente Decisión se adoptará de conformidad con el procedimiento contemplado en el artículo 58, apartado 2, de la Directiva (UE) 2016/680.

7. CONSIDERACIONES FINALES

(89) El Comité Europeo de Protección de Datos publicó su correspondiente dictamen ([94]), que se ha tenido en cuenta en la elaboración de la presente Decisión.

(90) La medida prevista en la presente Decisión se ajusta al dictamen del Comité creado en virtud del artículo 58 de la Directiva (UE) 2016/680.

(91) De conformidad con el artículo 6 *bis* del Protocolo (n.º 21) sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia, anejo al Tratado de la Unión Europea (TUE) y al Tratado de Funcionamiento de la Unión Europea (TFUE), no son vinculantes para Irlanda las normas establecidas en la Directiva (UE) 2016/680 y, por tanto, tampoco las establecidas en esta Decisión de Ejecución, relativas a tratamiento de datos personales por parte de los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación de la tercera parte, título V, capítulos 4 o 5, del TFUE en la medida en que no sean vinculantes para Irlanda las normas de la Unión que regulen formas de cooperación judicial en materia penal y de cooperación policial en cuyo marco deban respetarse las disposiciones establecidas sobre la base del artículo 16 del TFUE. Sin embargo, en virtud de la Decisión de Ejecución (UE) 2020/1745 del Consejo ([95]), la Directiva (UE) 2016/680 debe comenzar a aplicarse con carácter provisional en Irlanda a partir del 1 de enero de 2021. Irlanda, por tanto, está vinculada por la presente Decisión, en las mismas condiciones que rigen la aplicación de la Directiva (UE) 2016/680 en el país, tal como se establece en la Decisión de Ejecución (UE) 2020/1745 en lo que respecta a la parte del acervo de Schengen en que participa.

(92) De conformidad con lo dispuesto en los artículos 2 y 2 *bis* del Protocolo (n.º 22) sobre la posición de Dinamarca, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, Dinamarca no está sujeta por las normas establecidas en la Directiva (UE) 2016/680 y, por tanto, tampoco por las establecidas en esta Decisión de Ejecución, que se relacionan con el tratamiento de datos personales por parte de los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación de la tercera parte, título V, capítulos 4 o 5, del TFUE, ni está sujeta a su aplicación. Sin embargo, dado que la Directiva (UE) 2016/680 se basa en el acervo de Schengen, Dinamarca, de conformidad con el artículo 4 de dicho Protocolo, notificó el 26 de octubre de 2016 su decisión de aplicar la Directiva (UE) 2016/680. Por lo tanto, Dinamarca está obligada por el Derecho internacional a aplicar la presente Decisión de Ejecución.

(93) Por lo que se refiere a Islandia y Noruega, la presente Decisión constituye un desarrollo de las disposiciones del acervo de Schengen en el sentido del Acuerdo celebrado por el Consejo de la Unión Europea, la República de Islandia y el Reino de Noruega sobre la asociación de estos dos Estados a la ejecución, aplicación y desarrollo del acervo de Schengen ([96]).

(94) Por lo que respecta a Suiza, la presente Decisión constituye un desarrollo de las disposiciones del acervo de Schengen en el sentido del Acuerdo entre la Unión Europea, la Comunidad Europea y la Confederación Suiza sobre la asociación de la Confederación Suiza a la ejecución, aplicación y desarrollo del acervo de Schengen ([97]).

(95) Por lo que respecta a Liechtenstein, la presente Decisión constituye un desarrollo de las disposiciones del acervo de Schengen en el sentido del Protocolo entre la Unión Europea, la Comunidad Europea, la Confederación Suiza y el Principado de Liechtenstein sobre la adhesión del Principado de Liechtenstein al Acuerdo entre la Unión Europea, la Comunidad Europea y la Confederación Suiza sobre la asociación de la Confederación Suiza a la ejecución, aplicación y desarrollo del acervo de Schengen ([98]).

(96) Procede, por tanto, modificar la Decisión de Ejecución (UE) 2021/1773 en consecuencia.

([94]) Dictamen 27/2025 sobre el proyecto de Decisión de Ejecución de la Comisión Europea con arreglo a la Directiva (UE) 2016/680 sobre la protección adecuada de los datos personales por parte del Reino Unido, disponible en el siguiente enlace [en inglés] https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-272025-regarding-european-commission-draft_es.

([95]) Decisión de Ejecución (UE) 2020/1745 del Consejo, de 18 de noviembre de 2020, sobre la puesta en aplicación de las disposiciones del acervo de Schengen relativas a la protección de datos y sobre la puesta en aplicación provisional de determinadas disposiciones del acervo de Schengen en Irlanda (DO L 393 de 23.11.2020, p. 3, ELI: http://data.europa.eu/eli/dec_impl/2020/1745/oj).

([96]) Acuerdo celebrado por el Consejo de la Unión Europea con la República de Islandia y el Reino de Noruega sobre la asociación de estos dos Estados a la ejecución, aplicación y desarrollo del acervo de Schengen (DO L 176 de 10.7.1999, p. 36, ELI: http://data.europa.eu/eli/agree_internation/1999/439(1)/oj).

([97]) DO L 53 de 27.2.2008, p. 52.

([98]) DO L 160 de 18.6.2011, p. 21.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

El artículo 4 de la Decisión de Ejecución (UE) 2021/1773 se sustituye por el texto siguiente:

«*Artículo 4*

La presente Decisión tendrá validez hasta el 27 de diciembre de 2031, salvo que se prorrogue de conformidad con el procedimiento indicado en el artículo 58, apartado 2, de la Directiva (UE) 2016/680.».

Artículo 2

Los destinatarios de la presente Decisión son los Estados miembros.

Hecho en Bruselas, el 19 de diciembre de 2025.

Por la Comisión
Michael MCGRATH
Miembro de la Comisión