Consejo de la Unión Europea

Bruselas, 22 de enero de 2024
(OR. en)

5454/24

DATAPROTECT 23
JAI 62
RELEX 42

NOTA DE TRANSMISIÓN

De:	Por la secretaria general de la Comisión Europea, D.ª Martine DEPREZ, directora
A:	D.ª Thérèse BLANCHET, secretaria general del Consejo de la Unión Europea
N.° doc. Ción.:	COM(2024) 7 final
Asunto:	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

Adjunto se remite a las delegaciones el documento COM(2024) 7 final.

Adj.: COM(2024) 7 final

COMISIÓN
EUROPEA

Bruselas, 15.1.2024
COM(2024) 7 final

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

{SWD(2024) 3 final}

1. PRIMERA REVISIÓN: ANTECEDENTES Y CONTEXTO

El presente informe contiene las conclusiones de la Comisión sobre la primera revisión de las decisiones de adecuación adoptadas con arreglo al artículo 25, apartado 6, de la Directiva 95/46/CE[1] (Directiva sobre protección de datos).

En dichas decisiones, la Comisión concluyó que once países o territorios garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión Europea (UE)[2]: Andorra[3], Argentina[4], Canadá (para los operadores comerciales)[5], Guernesey[6], las Islas Feroe[7], la Isla de Man[8], Israel[9], Jersey[10], Nueva Zelanda[11], Suiza[12] y el Uruguay[13]. Por consiguiente, las transferencias de datos desde la UE a estos países o territorios pueden llevarse a cabo sin requisitos adicionales.

Cuando comenzó a aplicarse el Reglamento (UE) 2016/679[14] (RGPD) el 25 de mayo de 2018, se mantuvieron en vigor las decisiones de adecuación adoptadas en virtud de la Directiva

[1] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31).

[2] Tras su incorporación al Acuerdo sobre el Espacio Económico Europeo (EEE), el Reglamento General de Protección de Datos (RGPD) también se aplica a Noruega, Islandia y Liechtenstein. Las referencias a la UE contenidas en el presente informe deben entenderse en el sentido de que también abarcan a los Estados del EEE.

[3] Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la adecuada protección de los datos personales en Andorra (DO L 277 de 21.10.2010, p. 27).

[4] Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina (DO L 168 de 5.7.2003, p. 19).

[5] Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense *Personal Information and Electronic Documents Act* (DO L 2 de 4.1.2002, p. 13).

[6] Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003, relativa al carácter adecuado de la protección de los datos personales en Guernsey (DO L 308 de 25.11.2003, p. 27).

[7] Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada dada en la Ley de las Islas Feroe sobre el tratamiento de datos personales (DO L 58 de 9.3.2010, p. 17).

[8] Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004, relativa al carácter adecuado de la protección de los datos personales en la Isla de Man (DO L 151 de 30.4.2004, p. 48).

[9] Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por el Estado de Israel en lo que respecta al tratamiento automatizado de los datos personales (DO L 27 de 1.2.2011, p. 39).

[10] Decisión 2008/393/CE de la Comisión, de 8 de mayo de 2008, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales en Jersey (DO L 138 de 28.5.2008, p. 21).

[11] Decisión de Ejecución 2013/65/UE de la Comisión, de 19 de diciembre de 2012, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por Nueva Zelanda (DO L 28 de 30.1.2013, p. 12).

[12] Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa al nivel de protección adecuado de los datos personales en Suiza (DO L 215 de 25.8.2000, p. 1).

[13] Decisión de Ejecución 2012/484/UE de la Comisión, de 21 de agosto de 2012, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales (DO L 227 de 23.8.2012, p. 11).

[14] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de

sobre protección de datos[15]. Además, el RGPD ha aclarado que las decisiones de adecuación son «instrumentos vivos» y establece que la Comisión debe supervisar de manera continuada los acontecimientos producidos en terceros países que puedan afectar al funcionamiento de las decisiones de adecuación existentes[16]. Asimismo, el artículo 97 del RGPD exige a la Comisión que revise periódicamente estas decisiones (cada cuatro años) con el fin de determinar si los países y territorios que hayan recibido una decisión de adecuación siguen ofreciendo un nivel de protección de los datos personales adecuado.

Esta primera revisión de las decisiones de adecuación adoptadas en virtud del anterior marco de protección de datos de la UE se inició como parte de una evaluación más amplia de la aplicación y el funcionamiento del RGPD, sobre la que la Comisión presentó sus conclusiones en la Comunicación titulada «La protección de datos como pilar del empoderamiento de los ciudadanos y del enfoque de la UE para la transición digital: dos años de aplicación del Reglamento General de Protección de Datos»[17]. Sin embargo, la conclusión sobre este elemento de la revisión se aplazó para tener en cuenta la sentencia del Tribunal de Justicia en el asunto Schrems II[18], en la que el Tribunal aportó aclaraciones importantes sobre elementos clave de la norma de adecuación, así como otras novedades conexas. A su vez, esto dio lugar a intercambios detallados con los países y territorios implicados sobre aspectos pertinentes de su marco jurídico, sus mecanismos de control y su sistema de ejecución[19]. El presente informe tiene plenamente en cuenta todos estos acontecimientos, tanto los acaecidos en la UE como en los terceros países y territorios implicados.

Es importante señalar que esta primera revisión tiene lugar en un contexto de desarrollo exponencial de las tecnologías digitales. La importancia de las decisiones de adecuación ha aumentado considerablemente durante las últimas décadas, ya que los flujos de datos han pasado a ser un elemento integral de la transformación digital de la sociedad y de la globalización de la economía. La transferencia transfronteriza de datos se ha convertido en parte de las operaciones cotidianas de empresas europeas de todos los tamaños y pertenecientes a todos los sectores. Más que nunca, el respeto de la intimidad es fundamental para que los flujos comerciales sean estables, seguros y competitivos. En este contexto, las

---

estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).

[15] Véase el artículo 45, apartado 9, del RGPD, que establece que las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión adoptada de conformidad con los apartados 3 o 5 del artículo 45.

[16] Artículo 45, apartado 4, del RGPD. Véase también la sentencia del Tribunal de Justicia de la UE de 6 de octubre de 2015 en el asunto C-362/14, Maximillian Schrems/Data Protection Commissioner (Schrems I), ECLI:EU:C:2015:650, apartado 76.

[17] La Comunicación se publicó en junio de 2020 y se encuentra disponible en el siguiente enlace: https://ec.europa.eu/info/law/law-topic/data-protection/communication-two-years-application-general-data-protection-regulation_es.

[18] Sentencia del Tribunal de Justicia de la UE de 16 de julio de 2020 en el asunto C-311/18, Data Protection Commissioner / Facebook Ireland Limited y Maximillian Schrems (Schrems II), ECLI:EU:C:2020:559.

[19] La decisión de adecuación relativa a Japón se adoptó tomando como base el RGPD y prevé una revisión periódica independiente. La primera revisión se concluyó en abril de 2023 con el informe de la Comisión al Parlamento Europeo y al Consejo sobre la primera revisión del funcionamiento de la decisión de adecuación relativa a Japón [COM(2023) 275 final], disponible en el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=COM:2023:275:FIN.

decisiones de adecuación desempeñan un papel cada vez más importante en muchos aspectos. Al garantizar que la protección acompaña a los datos, se posibilita que los flujos de datos sean seguros y que respeten los derechos de las personas en consonancia con el enfoque para la transformación digital de la UE centrado en el ser humano. Al reconocer que el marco de privacidad de un tercer país proporciona un nivel de protección sustancialmente equivalente al de la UE, promueven la convergencia entre sistemas de privacidad basados en altos niveles de protección. Además, tal como se explica en el presente informe, en lugar de ser un «punto final», las decisiones de adecuación han sentado las bases para una cooperación más estrecha y una mayor convergencia normativa entre la UE y socios afines. Al permitir la libre circulación de datos personales, estas decisiones han abierto canales comerciales para los operadores de la UE, en particular al complementar y amplificar los beneficios de los acuerdos comerciales, además de facilitar la cooperación con socios extranjeros en una amplia gama de ámbitos normativos. Al ofrecer una solución sencilla y completa para las transferencias de datos, sin necesidad de que el exportador de datos facilite garantías adicionales u obtenga una autorización, facilitan el cumplimiento, en particular por parte de las pequeñas y medianas empresas, de los requisitos establecidos en el RGPD para las transferencias internacionales. Por último, gracias a su «efecto de red», las decisiones de adecuación adoptadas por la Comisión Europea son cada vez más importantes también fuera de la UE, ya que no solo permiten la libre circulación de datos con las treinta economías de la UE, sino también con muchas más jurisdicciones de todo el mundo[20] que reconocen a los países para los que existe una decisión de adecuación de la UE como «destinos seguros» con arreglo a sus propias normas de protección de datos.

Por todas estas razones, y tal como también confirma el intenso y fructífero diálogo mantenido con los terceros países o territorios implicados en el que se sustenta esta revisión, las decisiones de adecuación se han convertido en un componente estratégico de la relación general de la UE con estos socios extranjeros y se consideran un elemento facilitador importante para profundizar la cooperación en una amplia gama de ámbitos. Por lo tanto, es especialmente importante que estas decisiones sigan resultando apropiadas en un futuro y respondan a los nuevos acontecimientos y retos.

2. OBJETO Y METODOLOGÍA DE LA REVISIÓN

Las decisiones de adecuación examinadas en esta revisión se han adoptado con arreglo al marco de protección de datos de la UE previo al RGPD. Mientras que las decisiones más recientes se adoptaron hace aproximadamente una década (por ejemplo, las decisiones sobre Nueva Zelanda y el Uruguay, ambas de 2012), otras llevan más de veinte años en vigor (por ejemplo, las decisiones sobre Canadá, adoptada en 2001, y Suiza, adoptada en el año 2000). En este tiempo, los marcos de protección de datos de los once países y territorios han sufrido cambios, por ejemplo, debido a reformas legislativas o reglamentarias o a cambios en las prácticas de ejecución empleadas por las autoridades de protección de datos o en la jurisprudencia.

[20] Por ejemplo, Argentina, Colombia, Israel, Marruecos, Suiza y el Uruguay.

Al llevar a cabo su evaluación, la Comisión se ha centrado, por tanto, en los cambios en los marcos de protección de datos de los países y territorios pertinentes que han tenido lugar desde la adopción de la decisión de adecuación. Ha analizado la manera en que estos cambios han transformado el panorama de la protección de datos del país o territorio de que se trate y el hecho de si, teniendo en cuenta estos cambios, los distintos regímenes siguen garantizando un nivel de protección adecuado.

Para tal fin, se tuvieron plenamente en cuenta los cambios producidos en el propio régimen de protección de datos de la UE, en particular los derivados del comienzo de la aplicación del RGPD. En concreto, desde la adopción de estas decisiones de adecuación, se han aclarado con más detalle la norma jurídica aplicable a dichas decisiones y los elementos pertinentes para evaluar si un sistema extranjero garantiza un nivel de protección adecuado a través de la jurisprudencia del Tribunal de Justicia y las orientaciones adoptadas por el Grupo de Trabajo del Artículo 29 y su sucesor, el Comité Europeo de Protección de Datos[21] (CEPD).

Cabe destacar que, en su sentencia de 6 de octubre de 2015 en el asunto Schrems I, el Tribunal de Justicia estableció que, si bien no puede exigirse a un tercer país que asegure un nivel de protección idéntico al garantizado en la UE, debe entenderse que la prueba de adecuación exige un nivel de protección «sustancialmente equivalente»[22]. En particular, el Tribunal aclaró que 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, siempre que en la práctica demuestren ser eficaces para garantizar un nivel de protección adecuado[23]. Por lo tanto, la prueba de adecuación requiere una evaluación exhaustiva del sistema del tercer país en su totalidad que incluya el contenido de las medidas de protección de la privacidad y su aplicación y cumplimiento efectivos.

Además, el Tribunal aclaró que la evaluación de la Comisión no debe limitarse al marco general de protección de datos del tercer país, sino que también debe incluir las normas que rigen el acceso a los datos personales por parte de los poderes públicos, en particular con fines de aplicación de las leyes y de seguridad nacional[24]. Tomando la Carta de los Derechos Fundamentales como referencia, el Tribunal señaló varios requisitos que deben cumplir estas normas para ajustarse a la norma de la «equivalencia sustancial». Por ejemplo, la legislación en este ámbito debe establecer normas claras y precisas que regulen el alcance y la aplicación de una medida y que impongan unas exigencias mínimas, de modo que las personas cuyos datos personales resulten afectados dispongan de garantías suficientes que permitan proteger eficazmente sus datos contra el riesgo de abuso y contra cualquier acceso o utilización ilícitos[25]. También debe ofrecer a las personas la posibilidad de emprender acciones legales

[21] El Comité Europeo de Protección de Datos reúne a las autoridades de control de la protección de datos de los Estados miembros y al Supervisor Europeo de Protección de Datos.
[22] Schrems I, apartados 73, 74 y 96. Véase también el considerando 104 del Reglamento (UE) 2016/679, que hace referencia a la norma de la equivalencia sustancial.
[23] Schrems I, apartado 74.
[24] Schrems I, apartado 90.
[25] Schrems I, apartado 91.

para tener acceso a los datos personales que les conciernan o para lograr su rectificación o supresión[26].

El RGPD toma como base las aclaraciones facilitadas por el Tribunal de Justicia al establecer un catálogo detallado de elementos que la Comisión debe tener en cuenta a la hora de realizar una evaluación de la adecuación[27]. Además, en su sentencia de 16 de julio de 2020 en el asunto Schrems II, el Tribunal de Justicia profundizó en mayor medida en la norma de la «equivalencia sustancial», en particular en lo que respecta a las normas sobre el acceso a los datos personales por parte de los poderes públicos con fines de aplicación de las leyes y seguridad nacional. En concreto, aclaró que la norma de la «equivalencia sustancial» exige que los marcos jurídicos pertinentes que resultan vinculantes para los poderes públicos de los terceros países y territorios en cuestión incluyan garantías mínimas que aseguren que dichos poderes no puedan acceder a los datos más allá de lo necesario y proporcionado para perseguir objetivos legítimos, así como que los interesados gocen de derechos efectivos y exigibles contra dichos poderes[28].

La evolución de la norma de adecuación también se refleja en las orientaciones adoptadas originalmente por el Grupo de Trabajo del Artículo 29 y aprobadas posteriormente por el CEPD[29]. Estas orientaciones, y en especial las denominadas «referencias sobre adecuación», aclaran en mayor medida los elementos que debe tener en cuenta la Comisión a la hora de llevar a cabo una evaluación de la adecuación, en particular al proporcionar una visión general de las «garantías esenciales» para el acceso a los datos personales por parte de los poderes públicos. Dichas orientaciones se basan en particular en la jurisprudencia del Tribunal Europeo de Derechos Humanos, y el CEPD las actualizó para tener en cuenta las aclaraciones facilitadas por el Tribunal de Justicia en la sentencia Schrems II[30]. Es importante señalar que las referencias sobre la adecuación también reconocen que la norma de la «equivalencia sustancial» no implica una reproducción punto a punto («fotocopia») de las normas de la UE, dado que los medios para garantizar un nivel de protección comparable pueden variar en los distintos sistemas de privacidad, consecuencia de las distintas tradiciones jurídicas.

Por lo tanto, para determinar si las once decisiones de adecuación adoptadas en virtud de las normas anteriores siguen cumpliendo la norma establecida por el RGPD, la Comisión no solo ha tenido en cuenta los cambios producidos en los marcos de protección de datos de los países y territorios en cuestión, sino también la forma en que ha evolucionado la interpretación de la propia norma de adecuación con arreglo al Derecho de la UE. Esto incluye también una evaluación del marco jurídico que rige el acceso a —y el uso de— los datos personales transferidos desde la UE por parte de los poderes públicos de los países o territorios respecto

[26] Schrems I, apartado 95.
[27] Artículo 45, apartado 2, del RGPD.
[28] Schrems II, apartados 180 a 182.
[29] Referencias sobre adecuación, WP 254 rev. 01, 6 de febrero de 2018 (disponible en: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).
[30] Recomendaciones 02/2020 sobre las garantías esenciales europeas para medidas de vigilancia (disponibles en https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_es).

de los cuales se ha constatado que ofrecen un nivel de protección adecuado en virtud del artículo 25, apartado 6, de la Directiva sobre protección de datos.

3. PROCESO DE REVISIÓN

Tal como se ha explicado anteriormente, para cada uno de los países o territorios implicados, la evaluación de las decisiones de adecuación existentes abarca el marco de protección de datos y cualquier cambio producido en dicho marco jurídico desde que se adoptara la decisión de adecuación, así como las normas que rigen el acceso a los datos por parte de la administración, en particular para fines de aplicación de las leyes y seguridad nacional. Durante los últimos años, los servicios de la Comisión han tomado varias medidas para llevar a cabo esta evaluación, en estrecha cooperación con cada uno de los países o territorios pertinentes.

Para ayudar a la Comisión en sus obligaciones de seguimiento, cada uno de los once países o territorios le facilitó información exhaustiva sobre los cambios producidos en su régimen de protección de datos desde la adopción de la decisión de adecuación. Además, la Comisión solicitó información detallada a cada uno de los once países o territorios sobre las normas relativas al acceso a los datos personales por parte de la administración, en particular a efectos de aplicación de las leyes y seguridad nacional, que se aplican en dicho país o territorio. La Comisión también recopiló información de fuentes públicas, autoridades de control y encargadas del cumplimiento y expertos locales sobre el funcionamiento de las decisiones y sobre los cambios pertinentes en el Derecho y la práctica de cada uno de los países y territorios implicados, tanto en lo que se refiere a las normas de protección de datos aplicables a los operadores privados como en lo relativo al acceso por parte de la administración. Por último, en su caso, se han tenido debidamente en cuenta los compromisos internacionales suscritos por estos países o territorios en el marco de instrumentos regionales o universales.

Sobre esta base, la Comisión ha entablado un diálogo intenso con cada uno de los países y territorios en cuestión. En el contexto de este diálogo, muchos de dichos países y territorios han modernizado y reforzado su legislación en materia de privacidad a través de reformas generales o parciales (por ejemplo, Andorra, Canadá, las Islas Feroe, Suiza y Nueva Zelanda), impulsados, entre otros factores, por la necesidad de garantizar la continuidad de las decisiones de adecuación. Las autoridades de protección de datos de algunos de estos países han adoptado normativas u orientaciones para introducir nuevos requisitos de protección de datos (por ejemplo, Israel y el Uruguay) o para aclarar determinadas normas de privacidad (por ejemplo, Argentina, Canadá, Guernesey, Jersey, la Isla de Man, Israel y Nueva Zelanda), basándose en las prácticas de ejecución o la jurisprudencia. Además, con el fin de abordar las diferencias existentes en lo relativo al nivel de protección, se han negociado y acordado salvaguardias adicionales para los datos personales transferidos desde Europa con algunos de los países y territorios en cuestión, en aquellos casos en los que ha sido necesario para garantizar la continuidad de la decisión de adecuación. Por ejemplo, el Gobierno canadiense amplió los derechos de acceso y rectificación en lo relativo a los datos personales tratados por el sector público a todas las personas, independientemente de su nacionalidad o lugar de residencia (mientras que anteriormente estos derechos solo estaban disponibles para los

ciudadanos canadienses, los residentes permanentes o las personas físicamente presentes en Canadá)[31]. Otro ejemplo es el del Gobierno israelí, que introdujo salvaguardias específicas para reforzar la protección de los datos personales transferidos desde el Espacio Económico Europeo que en concreto crean nuevas obligaciones en términos de exactitud y conservación de los datos, refuerzan los derechos a la información y a la supresión e introducen categorías adicionales de datos sensibles[32].

Paralelamente, los servicios de la Comisión recabaron los puntos de vista del Parlamento Europeo (Comisión de Libertades Civiles, Justicia y Asuntos de Interior)[33], del Consejo (a través del Grupo «Protección de Datos»)[34], del CEPD[35] y del Grupo multilateral de expertos del RGPD[36] (que incluye a representantes de la sociedad civil, la industria, el mundo académico y los profesionales de la Justicia) sobre los avances de la evaluación, y les informaron regularmente al respecto.

El presente informe y el documento de trabajo de los servicios de la Comisión que lo acompaña son, por lo tanto, el resultado de una estrecha cooperación con cada uno de los países y territorios implicados, así como de la consulta con las instituciones y los organismos pertinentes de la UE y de las observaciones realizadas por estos. Se basan en diversas fuentes, como la legislación, los actos reglamentarios, la jurisprudencia, las decisiones y orientaciones de las autoridades de protección de datos, los informes de organismos de control (independientes) y las aportaciones de las partes interesadas. Antes de adoptarse el presente informe, se ha dado a todos los países y territorios anteriormente señalados la oportunidad de verificar la exactitud material de la información facilitada sobre su sistema en el documento de trabajo de los servicios de la Comisión.

4. PRINCIPALES RESULTADOS Y CONCLUSIONES

La primera revisión ha puesto de relieve que, desde la adopción de las decisiones de adecuación, los marcos de protección de datos vigentes en cada uno de los once países o territorios se han acercado en mayor medida al marco de la UE. Además, en lo relativo al acceso a los datos personales por parte de la administración, la primera revisión ha puesto de

[31] Artículo 12 de la Ley de Privacidad, Orden de Ampliación de la Ley de Privacidad n.º 1 y Orden de Ampliación de la Ley de Privacidad n.º 2.

[32] Reglamento 5783-2023 sobre la protección de la privacidad (instrucciones para los datos transferidos a Israel desde el Espacio Económico Europeo), publicado en el Boletín Oficial de Israel (*Reshumut*) el 7 de mayo de 2023.

[33] Véase, por ejemplo, la Resolución del Parlamento Europeo, de 25 de marzo de 2021, sobre el informe de evaluación de la Comisión sobre la ejecución del Reglamento General de Protección de Datos dos años después de su aplicación [2020/2717(RSP)], disponible en el siguiente enlace: https://eur-lex.europa.eu/legal-content/Es/TXT/?uri=CELEX%3A52021IP0111.

[34] Véanse, por ejemplo, la posición del Consejo y las conclusiones acerca de la aplicación del Reglamento General de Protección de Datos (RGPD), adoptadas el 19 de diciembre de 2019 y disponibles en el siguiente enlace: https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/en/pdf.

[35] Véase, por ejemplo, la contribución del CEPD a la evaluación del RGPD en virtud del artículo 97, adoptada el 18 de febrero de 2020 y disponible en el siguiente enlace: https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf.

[36] Véase, por ejemplo, el informe del Grupo multilateral de expertos sobre la evaluación del RGPD, disponible en el siguiente enlace: https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&do=groupDetail.groupMeeting&meetingId=21356.

manifiesto que el Derecho de estos países o territorios impone salvaguardias y limitaciones adecuadas y proporciona mecanismos de control y recurso en este sentido.

Las conclusiones detalladas relativas a cada uno de los once países o territorios se presentan en el documento de trabajo de los servicios de la Comisión que acompaña al presente informe. Sobre la base de estas conclusiones, la Comisión concluye que los once países y territorios siguen garantizando un nivel adecuado de protección para los datos personales transferidos desde la Unión Europea en el sentido del RGPD, según la interpretación del Tribunal de Justicia. A continuación, se resumen los resultados de cada uno de los países y territorios que se consideran adecuados.

4.1. Andorra

La Comisión acoge con satisfacción los cambios realizados en el marco jurídico andorrano desde la adopción de la decisión de adecuación, en concreto las modificaciones legislativas y las actividades de las autoridades de control. En particular, la adopción de la Ley cualificada 29/2021 sobre la protección de los datos personales, que entró en vigor en mayo de 2022, ha contribuido a aumentar el nivel de protección de datos, ya que dicha Ley está sumamente en consonancia con el RGPD en lo relativo a su estructura y a sus principales componentes.

En lo relativo al acceso a los datos personales por parte de la administración, los poderes públicos de Andorra están sujetos a normas claras, precisas y accesibles en virtud de las cuales dichos poderes pueden acceder a datos transferidos desde la UE y utilizarlos posteriormente para fines de interés público, en particular con fines de aplicación del Derecho penal y de seguridad nacional. Estas limitaciones y salvaguardias se derivan del marco jurídico general y los compromisos internacionales, en particular de la Constitución andorrana, el Convenio Europeo de Derechos Humanos (CEDH) y el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108 y Protocolo modificativo por el que se crea el Convenio 108+ modernizado), así como de normas específicas sobre la protección de datos aplicables al tratamiento de datos personales en el contexto de la aplicación de las leyes que esencialmente reproducen los elementos fundamentales de la Directiva (UE) 2016/680[37]. Además, el Derecho andorrano impone una serie de requisitos y limitaciones específicos para el acceso a los datos personales y su uso por parte de los poderes públicos y establece mecanismos de control y recurso en este ámbito.

Basándose en las conclusiones generales expuestas en el documento de trabajo de los servicios de la Comisión, la Comisión concluye que Andorra sigue garantizando un nivel de protección adecuado para los datos personales transferidos desde la UE.

Por lo que se refiere a las normas específicas sobre protección de datos que se aplican actualmente al tratamiento de datos por parte de los servicios de seguridad, la Comisión acoge

[37] 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.

con satisfacción la intención del legislador andorrano de sustituir estas normas por un régimen más amplio que se ajuste en mayor medida a las normas aplicables en la UE. La Comisión seguirá de cerca la futura evolución de la situación en este ámbito.

4.2. Argentina

La Comisión acoge con satisfacción los cambios realizados en el marco jurídico argentino desde la adopción de la decisión de adecuación, en concreto las modificaciones legislativas, la jurisprudencia y las actividades de las autoridades de control, que han contribuido a lograr un mayor nivel de protección de datos. En particular, se reforzó considerablemente la independencia de la autoridad argentina para el control de la protección de datos mediante el Decreto n.º 746/17, que encomienda a la Agencia de Acceso a la Información Pública (AAIP) la responsabilidad de controlar el cumplimiento de la normativa en materia de protección de datos. Además, la AAIP emitió una serie de reglamentos y dictámenes vinculantes que aclaran cómo debe interpretarse y aplicarse en la práctica el marco de protección de datos, contribuyéndose de este modo a mantener actualizada la normativa en materia de protección de datos. Argentina también reforzó sus compromisos internacionales en el ámbito de la protección de datos al adherirse en 2019 al Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y a su Protocolo adicional y al ratificar en 2023 el Protocolo modificativo por el que se crea el Convenio 108+ modernizado.

En lo relativo al acceso a los datos personales por parte de la administración, los poderes públicos de Argentina están sujetos a normas claras, precisas y accesibles en virtud de las cuales dichos poderes pueden acceder a datos transferidos desde la UE y utilizarlos posteriormente para fines de interés público, en particular con fines de aplicación del Derecho penal y seguridad nacional. Estas limitaciones y salvaguardias se derivan del marco jurídico general y los compromisos internacionales, en particular de la Constitución argentina, la Convención Americana sobre Derechos Humanos, el Convenio 108 y el Convenio 108+, así como de las normas argentinas sobre protección de datos (Ley 25.326 de Protección de los Datos Personales, de 4 de octubre de 2000) que también se aplican al tratamiento de datos personales por parte de los poderes públicos argentinos, especialmente con fines de aplicación de las leyes y seguridad nacional. Además, el Derecho argentino impone una serie de requisitos y limitaciones específicos para el acceso a los datos personales y su uso para fines de aplicación del Derecho penal y de seguridad nacional y establece mecanismos de control y recurso en este ámbito.

Basándose en las conclusiones generales expuestas en el documento de trabajo de los servicios de la Comisión, la Comisión concluye que Argentina sigue garantizando un nivel de protección adecuado para los datos personales transferidos desde la UE.

Asimismo, la Comisión recomienda consagrar en la legislación las protecciones que se han creado a nivel sublegislativo a fin de aumentar la seguridad jurídica y consolidar estos requisitos. El proyecto de ley sobre la protección de datos presentado recientemente en el Congreso argentino podría brindar la oportunidad de codificar estos avances y, de este modo,

reforzar aún más el marco de privacidad argentino. La Comisión seguirá de cerca la futura evolución de la situación en este ámbito.

4.3. Canadá

La Comisión acoge con satisfacción los cambios realizados en el marco jurídico canadiense desde la adopción de la decisión de adecuación, en concreto las diversas modificaciones legislativas, la jurisprudencia y las actividades de las autoridades de control, que han contribuido a lograr un mayor nivel de protección de datos. En particular, se ha reforzado la Ley de Protección de la Información Personal y Documentos Electrónicos (PIPEDA, por sus siglas en inglés) a través de diferentes modificaciones (por ejemplo, sobre las condiciones para la validez del consentimiento y las notificaciones de violación de la seguridad de los datos) y se han aclarado en mayor grado los requisitos clave en materia de protección de datos (por ejemplo, sobre el tratamiento de datos sensibles) a través de la jurisprudencia y de las orientaciones emitidas por la autoridad federal canadiense de protección de datos, la Oficina del Comisionado de Protección de la Vida Privada. Asimismo, la Comisión recomienda consagrar en la legislación algunas de las protecciones que se han creado a nivel sublegislativo a fin de aumentar la seguridad jurídica y consolidar estos requisitos. La reforma legislativa en curso de la PIPEDA podría ofrecer en concreto una oportunidad para codificar estos avances y, de este modo, seguir reforzando el marco canadiense de privacidad. La Comisión seguirá de cerca la futura evolución de la situación en este ámbito.

En lo relativo al acceso a los datos personales por parte de la administración, los poderes públicos de Canadá están sujetos a normas claras, precisas y accesibles en virtud de las cuales dichos poderes pueden acceder a datos transferidos desde la UE y utilizarlos posteriormente para fines de interés público, en particular con fines de aplicación del Derecho penal y de seguridad nacional. Estas limitaciones y salvaguardias se derivan del marco constitucional general (la Carta Canadiense de Derechos y Libertades), la jurisprudencia, la legislación específica que regula el acceso a los datos y las normas sobre protección de datos (es decir, la Ley de Privacidad y las leyes similares a nivel provincial) que también se aplican al tratamiento de datos personales por parte de los poderes públicos canadienses, especialmente con fines de aplicación de las leyes y seguridad nacional. Además, el sistema jurídico canadiense proporciona mecanismos de control y recurso eficaces en este ámbito, en particular mediante la reciente ampliación de los derechos de los interesados y de las posibilidades de recurso para los nacionales o residentes no canadienses.

Basándose en las conclusiones generales expuestas en el documento de trabajo de los servicios de la Comisión, la Comisión concluye que Canadá sigue garantizando un nivel de protección adecuado para los datos personales transferidos desde la UE a destinatarios sujetos a la PIPEDA. Tal como se ha señalado anteriormente, se está llevando a cabo una reforma legislativa de la PIPEDA que podría reforzar aún más la protección de la privacidad, en particular en ámbitos que son pertinentes para las decisiones de adecuación.

4.4. Islas Feroe

La Comisión acoge con satisfacción los cambios realizados en el marco jurídico feroés desde la adopción de la decisión de adecuación, en concreto las modificaciones legislativas, la jurisprudencia y las actividades de las autoridades de control, que han contribuido a lograr un mayor nivel de protección de datos. En particular, las Islas Feroe han modernizado considerablemente su marco de protección de datos mediante la adopción de la Ley de Protección de Datos, que entró en vigor en 2021 y acercó en gran medida el régimen feroés al RGPD.

En lo relativo al acceso a los datos personales por parte de la administración, los poderes públicos de las Islas Feroe están sujetos a normas claras, precisas y accesibles en virtud de las cuales dichos poderes pueden acceder a datos transferidos desde la UE y utilizarlos posteriormente para fines de interés público, en particular con fines de aplicación del Derecho penal y de seguridad nacional. Estas limitaciones y salvaguardias se derivan del marco jurídico general y los compromisos internacionales, en particular del marco constitucional y del CEDH, así como de leyes específicas que regulan el acceso a los datos por parte de la administración y de las normas de protección de datos que se aplican al tratamiento de datos personales con fines de aplicación del Derecho penal [Ley sobre el Tratamiento de Datos Personales por parte de los Servicios de Seguridad, que entró en vigor en las Islas Feroe en 2022 e integra en el Derecho feroés la legislación adoptada por Dinamarca para aplicar la Directiva (UE) 2016/680] y a efectos de seguridad nacional (contenidas en la Ley sobre el Servicio de Seguridad e Inteligencia). Además, existen mecanismos de control y recurso eficaces en este ámbito.

Basándose en las conclusiones generales expuestas en el documento de trabajo de los servicios de la Comisión, la Comisión concluye que las Islas Feroe siguen garantizando un nivel de protección adecuado para los datos personales transferidos desde la UE.

4.5. Guernesey

La Comisión acoge con satisfacción los cambios realizados en el marco jurídico de Guernesey desde la adopción de la decisión de adecuación, en concreto las modificaciones legislativas y las actividades de las autoridades de control, que han contribuido a lograr un mayor nivel de protección de datos. En particular, Guernesey ha modernizado considerablemente su marco de protección de datos mediante la adopción de la Ley de Protección de Datos (Bailía de Guernesey) de 2017, que se encuentra en vigor desde 2019 y acerca en gran medida el régimen de Guernesey al RGPD.

En lo relativo al acceso a los datos personales por parte de la administración, los poderes públicos de Guernesey están sujetos a normas claras, precisas y accesibles en virtud de las cuales dichos poderes pueden acceder a datos transferidos desde la UE y utilizarlos posteriormente para fines de interés público, en particular con fines de aplicación del Derecho penal y de seguridad nacional. Estas limitaciones y salvaguardias se derivan del marco jurídico general y los compromisos internacionales, en particular del CEDH y del Convenio 108, así como de las normas sobre protección de datos de Guernesey, especialmente las disposiciones específicas sobre el tratamiento de datos personales en el contexto de la aplicación de las leyes que se establecen en la Orden sobre Protección de Datos (Aplicación

de las Leyes y Cuestiones Conexas) (Bailía de Guernesey) de 2018. Además, el Derecho de Guernesey impone una serie de requisitos y limitaciones específicos para el acceso a los datos personales y su uso con fines de aplicación del Derecho penal y de seguridad nacional y establece mecanismos de control y recurso en este ámbito.

Basándose en las conclusiones generales expuestas en el documento de trabajo de los servicios de la Comisión, la Comisión concluye que Guernesey sigue garantizando un nivel de protección adecuado para los datos personales transferidos desde la UE.

4.6. Isla de Man

La Comisión acoge con satisfacción los cambios realizados en el marco jurídico manés desde la adopción de la decisión de adecuación, en concreto las modificaciones legislativas y las actividades de las autoridades de control, que han contribuido a lograr un mayor nivel de protección de datos. En concreto, en 2018, la Isla de Man adoptó nueva legislación [Ley de Protección de Datos de 2018, complementada por la Orden sobre Protección de Datos (Aplicación del RGPD) de 2018] que incorpora la mayoría de las disposiciones del marco de protección de datos de la UE al ordenamiento jurídico manés, realizándose únicamente pequeños ajustes en aspectos específicos, en particular para adaptar el marco al contexto local.

En lo relativo al acceso a los datos personales por parte de la Administración, los poderes públicos de la Isla de Man están sujetos a normas claras, precisas y accesibles en virtud de las cuales dichos poderes pueden acceder a datos transferidos desde la UE y utilizarlos posteriormente para fines de interés público, en particular con fines de aplicación del Derecho penal y de seguridad nacional. Estas limitaciones y salvaguardias se derivan del marco jurídico general y los compromisos internacionales, en particular del CEDH y del Convenio 108, así como de las normas sobre protección de datos de la Isla de Man, especialmente de las disposiciones específicas sobre el tratamiento de datos personales en el ámbito penal que se establecen en la Orden sobre Protección de Datos (Aplicación de la Directiva sobre protección de datos en el ámbito penal) de 2018 y en el Reglamento de 2018 por el que se aplica la Directiva sobre protección de datos en el ámbito penal. Además, el Derecho manés impone una serie de limitaciones específicas para el acceso a los datos personales y su uso para fines de aplicación del Derecho penal y seguridad nacional y establece mecanismos de control y recurso en este ámbito.

Basándose en las conclusiones generales expuestas en el documento de trabajo de los servicios de la Comisión, la Comisión concluye que la Isla de Man sigue garantizando un nivel de protección adecuado para los datos personales transferidos desde la UE.

4.7. Israel

La Comisión acoge con satisfacción los cambios realizados en el marco jurídico israelí desde la adopción de la decisión de adecuación, en concreto las modificaciones legislativas, la jurisprudencia y las actividades de las autoridades de control, que han contribuido a lograr un mayor nivel de protección de datos. En concreto, Israel introdujo salvaguardias específicas para reforzar la protección de los datos personales transferidos desde el Espacio Económico

Europeo mediante la adopción del Reglamento 5783-2023 sobre la Protección de la Privacidad (Instrucciones para los Datos Transferidos a Israel desde el Espacio Económico Europeo). Además, Israel reforzó los requisitos en materia de seguridad de los datos mediante la adopción del Reglamento 5777-2017 sobre la Protección de la Privacidad (Seguridad de los Datos) y consolidó la independencia de su autoridad de control de la protección de datos mediante una resolución gubernamental vinculante.

En lo relativo al acceso a los datos personales por parte de la administración, los poderes públicos de Israel están sujetos a normas claras, precisas y accesibles en virtud de las cuales dichos poderes pueden acceder a datos transferidos desde la UE y utilizarlos posteriormente para fines de interés público, en particular con fines de aplicación del Derecho penal y de seguridad nacional. Estas limitaciones y salvaguardias se derivan del marco jurídico general, en particular de la Ley Fundamental israelí, así como de la Ley 5741-1981 de Protección de la Privacidad y los Reglamentos adoptados en virtud de esta, que se aplican al tratamiento de datos personales por parte de los poderes públicos israelíes, especialmente con fines de aplicación de las leyes y seguridad nacional. Además, el Derecho israelí impone una serie de limitaciones específicas para el acceso a los datos personales y su uso para fines de aplicación del Derecho penal y de seguridad nacional y establece mecanismos de control y recurso en este ámbito.

Basándose en las conclusiones generales expuestas en el documento de trabajo de los servicios de la Comisión, la Comisión concluye que Israel sigue garantizando un nivel de protección adecuado para los datos personales transferidos desde la UE.

Asimismo, la Comisión recomienda consagrar en la legislación las protecciones que se han creado a nivel sublegislativo y a través de la jurisprudencia, con el fin de aumentar la seguridad jurídica y consolidar estos requisitos. El proyecto de Ley 5722-2022 sobre la Protección de la Privacidad (Enmienda n.º 14) presentado recientemente ante el Parlamento israelí ofrece una oportunidad importante para consolidar y codificar estos avances, con lo que se reforzaría en mayor medida el marco de privacidad israelí. La Comisión seguirá de cerca la futura evolución de la situación en este ámbito.

4.8. Jersey

La Comisión acoge con satisfacción los cambios realizados en el marco jurídico de Jersey desde la adopción de la decisión de adecuación, en concreto las modificaciones legislativas, la jurisprudencia y las actividades de las autoridades de control, que han contribuido a lograr un mayor nivel de protección de datos. En concreto, Jersey ha modernizado considerablemente su marco de protección de datos mediante la adopción de la Ley de Protección de Datos (Jersey) de 2018 y la Ley sobre la Autoridad de Protección de Datos (Jersey) de 2018, que entraron en vigor en 2018 y armonizan en gran medida el régimen de Jersey con el RGPD.

En lo relativo al acceso a los datos personales por parte de la administración, los poderes públicos de Jersey están sujetos a normas claras, precisas y accesibles en virtud de las cuales dichos poderes pueden acceder a datos transferidos desde la UE y utilizarlos posteriormente para fines de interés público, en particular con fines de aplicación del Derecho penal y de

seguridad nacional. Estas limitaciones y salvaguardias se derivan del marco jurídico general y los compromisos internacionales, en particular del CEDH y del Convenio 108, así como de las normas sobre protección de datos de Jersey, especialmente las disposiciones específicas sobre el tratamiento de datos personales en el contexto de la aplicación de las leyes que se establecen en la Ley de Protección de Datos (Jersey) de 2018, en su versión modificada a través del anexo 1 de dicha Ley. Además, el Derecho de Jersey impone una serie de limitaciones específicas para el acceso a los datos personales y su uso para fines de aplicación del Derecho penal y seguridad nacional y establece mecanismos de control y recurso en este ámbito.

Basándose en las conclusiones generales expuestas en el documento de trabajo de los servicios de la Comisión, la Comisión concluye que Jersey sigue garantizando un nivel de protección adecuado para los datos personales transferidos desde la UE.

4.9. Nueva Zelanda

La Comisión acoge con satisfacción los cambios realizados en el marco jurídico neozelandés desde la adopción de la decisión de adecuación, en concreto las modificaciones legislativas, la jurisprudencia y las actividades de las autoridades de control, que han contribuido a lograr un mayor nivel de protección de datos. En concreto, se llevó a cabo una reforma integral del régimen de protección de datos mediante la adopción de la Ley de Privacidad de 2020, que aumentó aún más la convergencia con el marco de protección de datos de la UE, en particular en lo que se refiere a las normas aplicables a las transferencias internacionales de datos personales y a los poderes de la autoridad de protección de datos (la Oficina del Comisionado de Privacidad).

En lo relativo al acceso a los datos personales por parte de la administración, los poderes públicos de Nueva Zelanda están sujetos a normas claras, precisas y accesibles en virtud de las cuales dichos poderes pueden acceder a datos transferidos desde la UE y utilizarlos posteriormente para fines de interés público, en particular con fines de aplicación del Derecho penal y de seguridad nacional. Estas limitaciones y salvaguardias se derivan del marco constitucional general (por ejemplo, la Ley sobre la Carta de Derechos) y la jurisprudencia, así como de las leyes específicas que regulan el acceso a los datos por parte de la administración y de las disposiciones de la Ley de Privacidad que también se aplican al tratamiento de datos personales por parte de las autoridades encargadas de la aplicación del Derecho penal y de la seguridad nacional. Además, el sistema jurídico neozelandés ofrece diferentes mecanismos de control y recurso en este ámbito.

Basándose en las conclusiones generales expuestas en el documento de trabajo de los servicios de la Comisión, la Comisión concluye que Nueva Zelanda sigue garantizando un nivel de protección adecuado para los datos personales transferidos desde la UE. La Comisión también acoge con satisfacción el hecho de que el Gobierno neozelandés haya presentado recientemente un proyecto de ley ante el Parlamento con miras a modificar la Ley de Privacidad de 2020 a fin de reforzar los requisitos de transparencia existentes. La Comisión seguirá de cerca la futura evolución de la situación en este ámbito.

4.10. Suiza

La Comisión acoge con satisfacción los cambios realizados en el marco jurídico suizo desde la adopción de la decisión de adecuación, en concreto las modificaciones legislativas, la jurisprudencia y las actividades de las autoridades de control, que han contribuido a lograr un mayor nivel de protección de datos. En particular, la Ley Federal de Protección de Datos actualizada ha aumentado aún más la convergencia con el marco de protección de datos de la UE, especialmente en lo que respecta a la protección de los datos sensibles y a las normas sobre las transferencias de datos internacionales. Asimismo, Suiza reforzó sus compromisos internacionales en el ámbito de la protección de datos mediante la ratificación del Convenio 108+ en septiembre de 2023.

En lo relativo al acceso a los datos personales por parte de la administración, los poderes públicos de Suiza están sujetos a normas claras, precisas y accesibles en virtud de las cuales dichos poderes pueden acceder a datos transferidos desde la UE y utilizarlos posteriormente para fines de interés público, en particular con fines de aplicación del Derecho penal y de seguridad nacional. Estas limitaciones y salvaguardias se derivan del marco jurídico general y los compromisos internacionales, en particular de la Constitución Federal de Suiza, del CEDH y del Convenio 108+, así como de las normas suizas en materia de protección de datos, especialmente la Ley Federal de Protección de Datos y las normas específicas sobre protección de datos que se aplican a las autoridades encargadas de la aplicación del Derecho penal (por ejemplo, el Código Procesal Penal) y de la seguridad nacional (por ejemplo, la Ley del Servicio de Inteligencia). Además, el Derecho suizo impone una serie de limitaciones específicas para el acceso a los datos personales y su uso para fines de aplicación del Derecho penal y seguridad nacional y establece mecanismos de control y recurso en este ámbito.

Basándose en las conclusiones generales expuestas en el documento de trabajo de los servicios de la Comisión, la Comisión concluye que Suiza sigue garantizando un nivel de protección adecuado para los datos personales transferidos desde la UE.

4.11. Uruguay

La Comisión acoge con satisfacción los cambios realizados en el marco jurídico uruguayo desde la adopción de la decisión de adecuación, en concreto las diversas modificaciones legislativas, la jurisprudencia y las actividades de las autoridades de control, que han contribuido a lograr un mayor nivel de protección de datos. En particular, el Uruguay actualizó y reforzó la Ley 18.331 de Protección de Datos Personales y la Acción de *Habeas Data* de 2008 mediante modificaciones legislativas realizadas en 2018 y 2020, con las que se amplió el alcance territorial de la legislación sobre protección de datos, se crearon nuevos requisitos de rendición de cuentas (como evaluaciones de impacto, la protección de datos desde el diseño y por defecto, la notificación de violaciones de la seguridad de los datos y el nombramiento de delegados de protección de datos) y se introdujeron protecciones adicionales para los datos biométricos. Además, el Uruguay reforzó sus compromisos internacionales en el ámbito de la protección de datos al adherirse al Convenio 108 en 2019 y al ratificar el Convenio 108+ en 2021.

En lo relativo al acceso a los datos personales por parte de la administración, los poderes públicos del Uruguay están sujetos a normas claras, precisas y accesibles en virtud de las cuales dichos poderes pueden acceder a datos transferidos desde la UE y utilizarlos posteriormente para fines de interés público, en particular con fines de aplicación del Derecho penal y de seguridad nacional. Estas limitaciones y salvaguardias se derivan del marco jurídico general y los compromisos internacionales, en particular de la Constitución uruguaya, la Convención Americana sobre Derechos Humanos, el Convenio 108 y el Convenio 108+, así como de las normas sobre protección de datos recogidas en la Ley 18.331 de Protección de Datos Personales y la Acción de *Habeas Data* que se aplican al tratamiento de datos personales por parte de los poderes públicos uruguayos, especialmente con fines de aplicación de las leyes y seguridad nacional. Además, el Derecho uruguayo impone una serie de requisitos y limitaciones específicos para el acceso a los datos personales y su uso por parte de los poderes públicos y establece mecanismos de control y recurso en este ámbito.

Basándose en las conclusiones generales extraídas como parte de esta primera revisión, la Comisión concluye que el Uruguay sigue garantizando un nivel de protección adecuado para los datos personales transferidos desde la UE.

5. SEGUIMIENTO Y COOPERACIÓN EN EL FUTURO

La Comisión reconoce y valora muy positivamente la excelente cooperación mantenida con las autoridades competentes de cada uno de los países y territorios implicados a la hora de llevarse a cabo esta revisión. La Comisión seguirá efectuando un estrecho seguimiento de los avances en los marcos de protección y la práctica real en los países y territorios en cuestión. En el caso de que en uno de los países o territorios considerados adecuados se produzcan cambios que afecten negativamente al nivel de protección de datos que se estima apropiado, la Comisión hará uso, cuando sea necesario, de las facultades que le confiere el artículo 45, apartado 5, del RGPD para suspender, modificar o revocar una decisión de adecuación.

La presente revisión confirma que la adopción de una decisión de adecuación no es un «punto final», sino que brinda la oportunidad de intensificar el diálogo y la cooperación con socios internacionales afines en lo relativo a los flujos de datos y las cuestiones digitales en general. En este sentido, la Comisión espera con interés la celebración de futuros intercambios con las autoridades competentes para seguir reforzando la cooperación a nivel internacional en lo relativo al fomento de unos flujos de datos seguros y libres, en particular mediante una cooperación reforzada en materia de ejecución. A fin de intensificar este diálogo y promover el intercambio de información y experiencias, la Comisión tiene la intención de organizar una reunión de alto nivel en 2024 que reúna a representantes de la UE y de todos los países para los que se haya emitido una decisión de adecuación.