**ACUERDO ENTRE LA UNIÓN EUROPEA, POR UNA PARTE, Y NUEVA ZELANDA, POR OTRA,
SOBRE EL INTERCAMBIO DE DATOS DE CARÁCTER PERSONAL ENTRE LA AGENCIA DE LA
UNIÓN EUROPEA PARA LA COOPERACIÓN POLICIAL (EUROPOL) Y LAS AUTORIDADES DE
NUEVA ZELANDA COMPETENTES EN MATERIA DE LUCHA CONTRA LA DELINCUENCIA
GRAVE Y EL TERRORISMO**

LA UNIÓN EUROPEA, denominada en lo sucesivo «Unión» o «UE»,

y

Nueva Zelanda,

denominadas conjuntamente en lo sucesivo «Partes contratantes»,

CONSIDERANDO QUE al autorizar el intercambio de datos personales entre la Agencia de la Unión Europea para la Cooperación Policial (Europol) y las autoridades competentes de Nueva Zelanda, el presente Acuerdo creará el marco para una cooperación operativa reforzada entre la Unión y Nueva Zelanda en el ámbito policial, salvaguardando al mismo tiempo los derechos humanos y las libertades fundamentales de todas las personas afectadas, incluidos el derecho a la intimidad y la protección de datos.

CONSIDERANDO QUE el presente Acuerdo se entiende sin perjuicio de los acuerdos de asistencia judicial mutua entre Nueva Zelanda y los Estados miembros de la Unión que permitan el intercambio de datos personales.

CONSIDERANDO QUE este acuerdo no impone a las autoridades competentes ningún requisito para la transferencia de datos personales y que la transferencia de datos personales solicitados en virtud del presente Acuerdo sigue siendo voluntaria.

RECONOCIENDO que las Partes contratantes aplican principios comparables de proporcionalidad y razonabilidad; la esencia común de tales principios es el requisito de garantizar un equilibrio justo entre todos los intereses afectados, ya sean públicos o privados, en vista de todas las circunstancias del caso en cuestión; dicho equilibrio implica, por un lado, el derecho a la intimidad de las personas junto con otros derechos e intereses humanos y, por otro lado, los objetivos legítimos compensatorios que pueden perseguirse, como los fines del tratamiento de datos personales reflejados en el presente Acuerdo.

HAN ACORDADO LO SIGUIENTE:

CAPÍTULO I

DISPOSICIONES GENERALES

ARTÍCULO 1

Objetivo

El objetivo del presente Acuerdo es permitir la transferencia de datos personales entre la Agencia de la Unión Europea para la Cooperación Policial (Europol) y las autoridades competentes de Nueva Zelanda para apoyar y reforzar la actuación de las autoridades de los Estados miembros de la Unión y de Nueva Zelanda, así como su cooperación mutua en la prevención y la lucha contra delitos, también respecto a la delincuencia grave y el terrorismo, al mismo tiempo que se garantizan salvaguardias apropiadas con respecto a los derechos humanos y las libertades fundamentales de las personas, incluido el derecho a la intimidad y la protección de datos.

ARTÍCULO 2

Definiciones

A efectos del presente Acuerdo, se entenderá por:

- 1) «Partes contratantes»: la Unión Europea y Nueva Zelanda;
- 2) «Europol»: Agencia de la Unión Europea para la Cooperación Policial, creada en virtud del Reglamento (UE) 2016/794 ⁽¹⁾ o cualquier modificación del mismo (en lo sucesivo, «Reglamento de Europol»);
- 3) «autoridades competentes»: en el caso de Nueva Zelanda, autoridades policiales nacionales que, bajo la legislación nacional de dicho país, son responsables de prevenir y combatir los delitos enumerados en el anexo II (en lo sucesivo, «autoridades competentes de Nueva Zelanda») y, en el caso de la Unión, Europol;
- 4) «organismos de la Unión»: las instituciones, entidades, misiones, oficinas y agencias creadas por o sobre la base del Tratado de la Unión Europea (TUE) y el Tratado de Funcionamiento de la Unión Europea (TFUE), enumerados en el anexo III;
- 5) «delitos»: los tipos de delitos enumerados en el anexo I y los delitos conexos; se considera que están relacionados con los tipos de delitos enumerados en el anexo I si se cometen con objeto de procurarse los medios para perpetrar, facilitar o cometer este tipo de delitos, o para garantizar la impunidad de quienes los cometan;
- 6) «datos personales»: toda información sobre un interesado;
- 7) «interesado»: una persona física identificada o identificable; es decir, una persona cuya identidad pueda determinarse, directa o indirectamente en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos datos de localización, un identificador en línea, uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;
- 8) «datos genéticos»: todos los datos personales relativos a las características genéticas de una persona que hayan sido heredadas o adquiridas, que proporcionen una información única sobre la fisiología o la salud de esa persona y que sean obtenidos en particular del análisis de una muestra biológica de la persona de que se trate;
- 9) «tratamiento»: cualquier operación o conjunto de operaciones, efectuadas o no con medios automáticos, aplicadas a datos personales o a conjuntos de datos personales, como la recogida, la anotación, la organización, la conservación, la adaptación o alteración, la extracción, la consulta, la utilización, la divulgación mediante transmisión, la difusión o cualquier otra forma puesta a disposición, la alineación o combinación, el bloqueo y la cancelación o destrucción;
- 10) «violación de la seguridad de los datos personales»: violación de la seguridad que ocasione, de forma accidental o ilícita, la destrucción, la pérdida o alteración, la comunicación no autorizada o el acceso a datos personales transmitidos, conservados o tratados de otra forma;
- 11) «autoridad de control»: una o varias autoridades nacionales independientes que son, por separado o en conjunto, responsables de la protección de datos de conformidad con el artículo 16 y que han sido notificadas de conformidad con dicho artículo; es posible que esto incluya a aquellas autoridades cuya responsabilidad abarque también otros derechos humanos;
- 12) «organización internacional»: una organización y sus organismos subordinados de Derecho internacional público, o cualquier otro organismo creado por, o sobre la base de un acuerdo entre dos o más países.

ARTÍCULO 3

Finalidades del tratamiento de datos personales

1. Los datos personales solicitados y recibidos en virtud del presente Acuerdo serán tratados únicamente con fines de prevención, investigación, detección o enjuiciamiento de delitos o de ejecución de sanciones penales, dentro de los límites del artículo 4, apartado 5, y de los mandatos respectivos de las autoridades competentes.

⁽¹⁾ Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo (DO L 135 de 24.5.2016, p. 53).

2. Las autoridades competentes indicarán claramente, a más tardar en el momento de la transferencia de datos personales, el fin o los fines específicos para los que se están transfiriendo los datos. Para transferencias a Europol, el fin o fines de dicha transferencia se especificarán de acuerdo con el fin o los fines específicos de tratamiento establecidos en el mandato de Europol.

CAPÍTULO II

INTERCAMBIO DE INFORMACIÓN Y PROTECCIÓN DE DATOS

ARTÍCULO 4

Principios generales en materia de protección de datos

1. Cada Parte contratante dispondrá que los datos personales intercambiados en virtud del presente Acuerdo sean:
 - a) tratados de manera leal, lícita y exclusivamente para el fin o los fines para los que hayan sido transferidos de conformidad con el artículo 3;
 - b) adecuados, pertinentes y limitados a lo necesario en relación con el fin o los fines para los que son tratados;
 - c) exactos y actualizados, para lo que cada Parte contratante dispondrá que las autoridades competentes tomen todas las medidas razonables para garantizar que los datos personales que sean inexactos con respecto a los fines para los que son tratados se rectifiquen o supriman sin demora injustificada;
 - d) conservados en una forma que permita identificar a los interesados durante un período no superior al necesario para los fines para los que se someten a tratamiento;
 - e) tratados de un modo que garantice una seguridad adecuada de los datos personales.
2. La autoridad competente transmisora podrá indicar, en el momento de la transferencia de los datos personales, cualquier limitación del acceso a los mismos o el uso que deba hacerse de ellos, en términos generales o específicos, también en lo que se refiere a su transferencia ulterior, supresión o destrucción después de un determinado período de tiempo, o al tratamiento ulterior de los mismos. Cuando la necesidad de tales limitaciones se manifieste después de que se hayan facilitado los datos personales, la autoridad competente transmisora informará de ello a la autoridad receptora.
3. Cada Parte contratante garantizará que la autoridad competente receptora cumpla cualquier restricción de acceso o de ulterior utilización de los datos personales indicada por la autoridad competente transmisora, tal como se describe en el apartado 2.
4. Cada Parte contratante dispondrá que sus autoridades competentes apliquen las medidas técnicas y organizativas apropiadas para poder demostrar que el tratamiento será conforme con el presente Acuerdo y que se protegerán los derechos de los interesados afectados.
5. Cada Parte contratante garantizará que las autoridades competentes no transfieran los datos personales que se hayan obtenido en vulneración manifiesta de los derechos humanos reconocidos por las normas de Derecho internacional vinculantes para las Partes contratantes. Cada Parte contratante garantizará que los datos personales recibidos no se utilizarán para solicitar, dictar o ejecutar la pena capital u otra forma de trato cruel o inhumano.
6. Cada Parte contratante garantizará que se lleve un registro de todas las transferencias de datos personales con arreglo al presente Acuerdo y del fin o los fines de dichas transferencias.

ARTÍCULO 5

Categorías especiales de datos personales y categorías diferentes de interesados

1. Queda prohibida la transferencia de datos personales de víctimas de delitos, testigos u otras personas que pudieran facilitar información sobre infracciones penales, así como de menores de dieciocho años, a menos que la transferencia sea estrictamente necesaria, razonable y proporcionada en casos concretos para prevenir o combatir un delito.

2. La transferencia de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud, a la vida sexual o a las orientaciones sexuales de una persona física solo se permitirá cuando sea estrictamente necesario, razonable y proporcionado en casos individuales para prevenir o combatir un delito y si dichos datos, salvo los datos biométricos, complementan otros datos personales.

3. Las Partes contratantes garantizarán que el tratamiento de datos personales en virtud de los apartados 1 y 2 del presente artículo esté sujeto a salvaguardias adicionales ante riesgos específicos, entre ellas las restricciones de acceso, las medidas para la seguridad de los datos en el sentido del artículo 15 y las limitaciones a las transferencias ulteriores en virtud del artículo 7.

ARTÍCULO 6

Tratamiento automatizado de datos personales

Quedan prohibidas las decisiones basadas únicamente en un tratamiento automatizado de los datos personales intercambiados, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o le afecten significativamente, salvo que la ley lo autorice para la prevención y lucha contra delitos, y que ofrezca garantías adecuadas para salvaguardar los derechos y libertades del interesado, incluido al menos el derecho a obtener la intervención humana.

ARTÍCULO 7

Transferencia ulterior de los datos personales recibidos

1. Nueva Zelanda garantizará que sus autoridades competentes solo transfieran datos personales recibidos en virtud del presente Acuerdo a otras autoridades de Nueva Zelanda si:

- a) Europol ha dado su autorización explícita previa;
- b) el fin o los fines de la transferencia ulterior son los mismos que el fin o los fines originales de la transferencia por parte de Europol o están directamente relacionados, dentro de los límites del artículo 3, apartado 1, con dichos fin o fines originales;
- c) la transferencia ulterior está sujeta a las mismas condiciones y garantías que las aplicables a la transferencia original.

Sin perjuicio de lo dispuesto en el artículo 4, apartado 2, no se requerirá autorización previa cuando la autoridad receptora sea ella misma una autoridad competente de Nueva Zelanda. Lo mismo se aplica a la capacidad de Europol de compartir datos personales con las autoridades responsables en los Estados miembros de la Unión de la prevención y la lucha contra delitos, y con los organismos de la Unión.

2. Nueva Zelanda garantizará que se prohíban las transferencias ulteriores de datos personales recibidos por sus autoridades competentes en virtud del presente Acuerdo a las autoridades de un tercer país o a una organización internacional, a menos que se cumplan las siguientes condiciones:

- a) la transferencia se refiere a datos personales distintos a los contemplados en el artículo 5;
- b) Europol ha dado su autorización explícita previa;
- c) el fin o los fines de la transferencia ulterior son los mismos que el fin o los fines originales de la transferencia por parte de Europol, y
- d) la transferencia ulterior está sujeta a las mismas condiciones y garantías que las aplicables a la transferencia original.

3. Europol solo podrá conceder su autorización con arreglo al apartado 2, letra b), del presente artículo para una transferencia ulterior a la autoridad de un tercer país o a una organización internacional si, y en la medida en que exista una decisión de adecuación, un acuerdo internacional que ofrezca garantías adecuadas con respecto a la protección del derecho a la intimidad y los derechos y libertades fundamentales de las personas, un acuerdo de cooperación o cualquier otro fundamento jurídico para las transferencias de datos personales el sentido del Reglamento de Europol que regule la transferencia ulterior.

4. La Unión garantizará que se prohíban las transferencias ulteriores de datos personales recibidos por parte de Europol en virtud del presente Acuerdo a los organismos de la Unión no enumerados en el anexo III, a las autoridades de terceros países o a una organización internacional, a menos que:
- la transferencia se refiera a datos personales distintos de los contemplados en el artículo 5;
 - Nueva Zelanda haya dado su autorización explícita previa;
 - el fin o los fines de la transferencia ulterior sean los mismos que el fin o los fines originales de la transferencia por parte de Nueva Zelanda, y
 - haya vigente una decisión de adecuación, un acuerdo internacional que ofrezca salvaguardias adecuadas con respecto a la protección del derecho a la intimidad y de los derechos y libertades fundamentales de las personas o un acuerdo de cooperación en el sentido del Reglamento de Europol con ese tercer país u organización internacional o a menos que Europol pueda basarse en cualquier otra base legal para las transferencias de datos personales en el sentido del Reglamento de Europol.

ARTÍCULO 8

Valoración de la fiabilidad de la fuente y la exactitud de la información

- Las autoridades competentes indicarán, en la medida de lo posible, a más tardar en el momento de la transferencia de datos personales, la fiabilidad de la fuente de información sobre la base de uno o varios de los criterios siguientes:
 - cuando no quepa duda sobre la autenticidad, veracidad y competencia de la fuente, o si la información es suministrada por una fuente que en el pasado haya resultado ser fiable en todos los casos;
 - cuando la información sea facilitada por una fuente que en el pasado haya resultado ser fiable en la mayoría de los casos;
 - cuando la información sea facilitada por una fuente que haya resultado ser poco fiable en la mayoría de los casos;
 - cuando no pueda determinarse la fiabilidad de la fuente.
- Las autoridades competentes indicarán, en la medida de lo posible, a más tardar en el momento de la transferencia de datos personales, la exactitud de la información sobre la base de uno o varios de los criterios siguientes:
 - información cuya exactitud no se ponga en duda en el momento de la transferencia;
 - información conocida personalmente por la fuente, pero no conocida personalmente por el funcionario que la transmite;
 - información no conocida personalmente por la fuente, pero corroborada por otra información ya registrada;
 - cuando la información no sea conocida personalmente por la fuente y no pueda ser corroborada.
- Cuando la autoridad competente receptora, sobre la base de la información que ya posee, llegue a la conclusión de que se debe corregir la evaluación de la información facilitada por la autoridad competente transmisora o de su fuente, de conformidad con los apartados 1 y 2, informará a dicha autoridad competente e intentará acordar una modificación de dicha evaluación. La autoridad competente receptora no modificará la evaluación de la información recibida o de su fuente sin tal acuerdo.
- Si una autoridad competente recibe información sin una evaluación, tratará de evaluar, en la medida de lo posible y de acuerdo con la autoridad competente transmisora, la fiabilidad de la fuente o la exactitud de la información sobre la base de los datos que ya obren en su poder.
- Si no se puede hacer una evaluación fiable, la información se evaluará de conformidad con el apartado 1, letra d), y el apartado 2, letra d), según proceda.

DERECHOS DE LOS INTERESADOS**ARTÍCULO 9****Derecho de acceso**

1. Las Partes contratantes garantizarán que el interesado tenga derecho a obtener información, a intervalos razonables, sobre si los datos personales que le conciernen se tratan en el marco del presente Acuerdo y, en su caso, el acceso al menos a la siguiente información:

- a) confirmación de si se están tratando o no datos que guarden relación con su persona;
- b) información sobre, al menos, el fin o los fines del tratamiento, las categorías de datos implicadas y, en su caso, los destinatarios o categorías de destinatarios a quienes se divulguen los datos;
- c) la existencia del derecho a solicitar a la autoridad competente la rectificación, corrección, supresión o eliminación de los datos personales relativos al interesado, o la limitación de su tratamiento;
- d) indicación de la base jurídica con arreglo a la cual se realizará el tratamiento;
- e) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
- f) comunicación en forma inteligible de los datos personales objeto de tratamiento y de cualquier información disponible sobre el origen de los datos.

2. En los casos en que se ejerza el derecho de acceso, se consultará a la Parte contratante que realiza la transferencia sobre una base no vinculante antes de que se adopte una decisión definitiva sobre la solicitud de acceso.

3. Las Partes contratantes podrán disponer que el suministro de información en respuesta a cualquier solicitud con arreglo al apartado 1 se retrase, deniegue o limite en la medida y durante el tiempo en que dicha denegación o limitación constituya una medida necesaria, razonable y proporcionada, teniendo en cuenta los derechos e intereses fundamentales del interesado, con el fin de:

- a) garantizar que no se pongan en peligro ninguna investigación ni enjuiciamiento penal;
- b) proteger los derechos y libertades de terceros, o
- c) proteger la seguridad nacional y el orden público y prevenir delitos.

4. Las Partes contratantes garantizarán que la autoridad competente informe por escrito al interesado de cualquier retraso, denegación o restricción de acceso y de los motivos de tal retraso, denegación o restricción de acceso. Dichos motivos podrán omitirse cuando ello menoscabe la finalidad del retraso, la denegación o la restricción con arreglo al apartado 3. La autoridad competente informará al interesado de las posibilidades de presentar una reclamación ante las autoridades de control respectivas y de otras vías de recurso disponibles previstas en sus respectivos marcos jurídicos.

ARTÍCULO 10**Derecho de rectificación, corrección, supresión, eliminación y restricción**

1. Las Partes contratantes garantizarán que todo interesado tenga derecho a solicitar a las autoridades competentes que rectifiquen o corrijan los datos personales inexactos relativos al interesado y que hayan sido transferidos en virtud del presente Acuerdo. Teniendo en cuenta el fin o los fines del tratamiento, esto incluye el derecho a que se completen los datos personales incompletos transferidos en virtud del presente Acuerdo.

2. La rectificación y corrección incluirá la supresión y eliminación de datos personales que ya no sean necesarios para el fin o los fines para los que se tratan.

3. Las Partes contratantes podrán prever la restricción del tratamiento en lugar de la supresión y eliminación de los datos personales en caso de que hubiera motivos razonables para suponer que la supresión y eliminación podrían perjudicar intereses legítimos del interesado.

4. Las autoridades competentes se informarán mutuamente de las medidas tomadas en virtud de los apartados 1, 2 y 3. La autoridad competente receptora rectificará, corregirá, suprimirá o restringirá el tratamiento de conformidad con las medidas adoptadas por la autoridad competente transmisora.
5. Las Partes contratantes dispondrán que la autoridad competente que haya recibido la petición informe al interesado por escrito, sin demora indebida, y en cualquier caso en el plazo de tres meses a partir de la recepción de una solicitud de conformidad con los apartados 1 o 2, de que los datos que le conciernen han sido rectificadas, corregidos, suprimidos, eliminados o restringidos en su tratamiento.
6. Las Partes contratantes dispondrán que la autoridad competente que haya recibido la solicitud informe por escrito al interesado sin demora indebida y en cualquier caso en el plazo de tres meses a partir de la recepción de la solicitud de cualquier denegación de rectificación, corrección, supresión, eliminación o restricción del tratamiento, de las razones de dicha denegación y de la posibilidad de presentar una reclamación ante las autoridades de control respectivas y de otras vías de recurso disponibles en los marcos jurídicos respectivos.

ARTÍCULO 11

Notificación de una violación de la seguridad de datos personales a las autoridades afectadas

1. Las Partes contratantes garantizarán, en el caso de una violación de la seguridad de los datos personales que afecte a los datos personales transferidos en virtud del presente Acuerdo, que las respectivas autoridades competentes se notifiquen entre sí dicha violación de la seguridad de los datos personales sin demora, así como a su respectiva autoridad de control, y adopten medidas para mitigar sus posibles efectos adversos.
2. La notificación deberá, como mínimo:
 - a) describir la naturaleza de la violación de la seguridad de los datos personales, incluidos, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
 - b) describir las posibles consecuencias de la violación de la seguridad de datos personales;
 - c) describir las medidas adoptadas o propuestas por la autoridad competente para poner remedio a la violación de la seguridad de los datos personales, incluidas las medidas adoptadas para mitigar los posibles efectos negativos.
3. En la medida en que no sea posible facilitar toda la información requerida al mismo tiempo, podrá facilitarse por fases. La información pendiente se facilitará sin más demora injustificada.
4. Las Partes contratantes garantizarán que sus respectivas autoridades competentes documenten toda violación de la seguridad de los datos personales que afecte a datos personales transferidos en virtud del presente Acuerdo, incluidos los hechos relativos a la violación de la seguridad de los datos personales, sus efectos y las medidas correctoras adoptadas, permitiendo así a su respectiva autoridad de control verificar el cumplimiento de los requisitos legales aplicables.

ARTÍCULO 12

Comunicación de una violación de la seguridad de los datos personales al interesado

1. Las Partes contratantes dispondrán que, cuando sea probable que una violación de la seguridad de los datos personales a que se refiere el artículo 11 tenga un efecto adverso grave para los derechos y libertades del interesado, sus respectivas autoridades competentes comuniquen al interesado, sin dilación indebida, la violación de la seguridad de los datos personales.
2. En la comunicación al interesado según lo dispuesto en el apartado 1 se describirá, a ser posible, la naturaleza de la violación de la seguridad de los datos personales, se recomendarán medidas para mitigar los posibles efectos adversos de la violación de la seguridad de los datos personales y, además, se proporcionarán el nombre y la información de contacto del punto de contacto de quien se puede obtener más información.
3. La comunicación al interesado en virtud del apartado 1 no será necesaria si:
 - a) los datos personales afectados por la violación han sido objeto de medidas de protección tecnológica adecuadas que hacen ininteligibles los datos para cualquier persona que no esté autorizada a acceder a dichos datos;

- b) se han tomado medidas posteriores que garantizan que ya no sea probable que los derechos y libertades del interesado se vean gravemente afectados, o
- c) la comunicación al interesado en virtud del apartado 1 supone una carga desproporcionada, en particular habida cuenta del número de casos afectados; en este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva al interesado.

4. La comunicación al interesado en virtud del apartado 1 podrá retrasarse, restringirse u omitirse cuando sea probable que dicha comunicación:

- a) obstruya indagaciones, investigaciones o procedimientos administrativos o judiciales;
- b) perjudique la prevención, detección, investigación y enjuiciamiento de delitos o la ejecución de sanciones penales, el orden público o la seguridad nacional;
- c) afecte a los derechos y libertades de terceros;

siempre y cuando ello sea una medida necesaria y proporcionada, teniendo debidamente en cuenta los intereses legítimos del interesado de que se trate.

ARTÍCULO 13

Conservación, revisión, corrección y supresión de datos personales

1. Las Partes contratantes dispondrán que se establezcan plazos adecuados para la conservación de los datos personales recibidos en virtud del presente Acuerdo o para la revisión periódica de la necesidad de conservación de datos personales, de modo que dichos datos personales no se conserven más tiempo del necesario para el fin o los fines para los que se transfieren.

2. En cualquier caso, la necesidad de seguir conservando datos personales se revisará a más tardar tres años después de su transferencia y, si no se adopta ninguna decisión justificada y documentada sobre la continuación de la conservación de los datos personales, dichos datos personales se suprimirán automáticamente transcurridos tres años.

3. Cuando una autoridad competente tenga motivos para creer que los datos personales anteriormente transferidos por ella son incorrectos, inexactos, han dejado de estar actualizados o no deberían haber sido transmitidos, informará de ello a la autoridad competente receptora, quien corregirá o suprimirá dichos datos y lo notificará a la autoridad competente transmisora.

4. Cuando una autoridad competente tenga motivos para creer que los datos personales anteriormente recibidos son incorrectos, inexactos, han dejado de estar actualizados o no deberían haber sido transmitidos, informará de ello a la autoridad competente transmisora, quien expondrá su posición al respecto. Cuando la autoridad competente transmisora llegue a la conclusión de que los datos personales son incorrectos, inexactos, han dejado de estar actualizados o no deberían haber sido transmitidos, informará de ello a la autoridad competente receptora, quien corregirá o suprimirá dichos datos y lo notificará a la autoridad competente transmisora.

ARTÍCULO 14

Registro y documentación

1. Las Partes contratantes dispondrán la conservación de registros y documentación de la recogida, la modificación, el acceso, la divulgación, incluidas las transferencias posteriores, la combinación y la supresión de datos personales.

2. Los registros o la documentación a que se refiere el apartado 1 se pondrán a disposición de la autoridad de control respectiva previa solicitud para la verificación de la legalidad del tratamiento, el autocontrol y la garantía de la integridad y seguridad adecuadas de los datos.

ARTÍCULO 15

Seguridad de los datos

1. Las Partes contratantes garantizarán la aplicación de medidas técnicas y organizativas para proteger los datos personales intercambiados en virtud del presente Acuerdo.
2. En lo que respecta al tratamiento automatizado, las Partes contratantes garantizarán la aplicación de medidas destinadas a:
 - a) denegar a las personas no autorizadas el acceso a los equipamientos utilizados para el tratamiento de datos personales (control del acceso a los equipamientos);
 - b) impedir la lectura, copia, modificación o retirada no autorizadas de los soportes de datos (control de los soportes de datos);
 - c) impedir que se introduzcan sin autorización datos personales y que datos personales conservados se inspeccionen, modifiquen o supriman sin autorización (control del almacenamiento);
 - d) impedir que los sistemas de tratamiento automatizado puedan ser utilizados por personas no autorizadas por medio de equipamientos de transmisión de datos (control del usuario);
 - e) garantizar que las personas autorizadas para utilizar un sistema de tratamiento automatizado solo puedan tener acceso a los datos personales para los que han sido autorizados (control del acceso a los datos);
 - f) garantizar la posibilidad de verificar y determinar a qué organismos pueden transmitirse o se han transmitido datos personales utilizando equipamientos de transmisión de datos (control de la transmisión);
 - g) garantizar la posibilidad de verificar y determinar qué datos personales se han introducido en los sistemas de tratamiento automatizado, en qué momento y por quién (control de la introducción);
 - h) garantizar que sea posible verificar y establecer qué miembro del personal ha accedido a qué datos personales y a qué hora (registro de acceso);
 - i) impedir que durante las transferencias de datos personales o durante el transporte de soportes de datos, los datos personales puedan ser leídos, copiados, modificados o suprimidos sin autorización (control del transporte);
 - j) garantizar que los sistemas instalados puedan repararse rápidamente en caso de avería (restablecimiento);
 - k) garantizar que las funciones del sistema no presenten defectos, que los errores de funcionamiento se señalen de forma inmediata (fiabilidad) y que los datos personales conservados no se falseen por defectos de funcionamiento del sistema (autenticidad).

ARTÍCULO 16

Autoridad de control

1. Cada Parte contratante garantizará que una autoridad pública independiente responsable de la protección de datos (autoridad de control) supervise aquellos asuntos que afectan al derecho a la intimidad de las personas, incluidas las normas nacionales relevantes en virtud del presente Acuerdo, para proteger los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos personales. Las Partes contratantes se notificarán mutuamente la autoridad que cada una de ellas considere como autoridad de control.
2. Las Partes contratantes garantizarán que cada autoridad de control:
 - a) actúe con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes; dicha autoridad actuará sin influencia externa y no solicitará ni aceptará instrucciones; sus miembros tendrán un mandato seguro, que incluya garantías contra la destitución arbitraria;
 - b) disponga de los recursos humanos, técnicos y financieros, así como de los locales e infraestructuras necesarios para el desempeño efectivo de sus funciones y el ejercicio de sus competencias;
 - c) disponga de poderes efectivos de investigación e intervención para supervisar los organismos que supervisa y para emprender acciones judiciales;
 - d) esté facultada para conocer de las reclamaciones de particulares sobre el uso de sus datos personales por las autoridades competentes bajo su supervisión.

ARTÍCULO 17

Recursos administrativos y judiciales

Los interesados tendrán derecho a un recurso administrativo y judicial efectivo en caso de violación de los derechos y garantías reconocidos en el presente Acuerdo como consecuencia del tratamiento de sus datos personales. Las Partes contratantes se notificarán mutuamente la legislación nacional que cada una de ellas considere que establece los derechos garantizados en virtud del presente artículo.

CAPÍTULO III

DIFERENCIAS

ARTÍCULO 18

Solución de diferencias

Todas las diferencias que puedan surgir en relación con la interpretación, aplicación o ejecución del presente Acuerdo, así como cualquier asunto relacionado con el mismo, darán lugar a consultas y negociaciones entre representantes de las Partes contratantes con vistas a alcanzar una solución mutuamente aceptable.

ARTÍCULO 19

Cláusula suspensiva

1. En caso de incumplimiento grave o incumplimiento de las obligaciones derivadas del presente Acuerdo, las Partes contratantes podrán suspender el presente Acuerdo de forma temporal parcialmente o por completo mediante notificación escrita a la otra Parte contratante por vía diplomática. Dicha notificación por escrito no podrá efectuarse hasta después de que las Partes contratantes hayan abierto un período razonable de consulta sin llegar a una resolución, y la suspensión entrará en vigor veinte días después de la fecha de recepción de dicha notificación. Dicha suspensión podrá ser levantada por la Parte contratante que lo suspenda previa notificación por escrito a la otra Parte contratante. El levantamiento de la suspensión tendrá lugar inmediatamente después de la recepción de la citada notificación.
2. No obstante la suspensión del presente Acuerdo, los datos personales que entren en el ámbito de su aplicación y hayan sido transferidos con anterioridad a la suspensión del presente Acuerdo seguirán tratándose de conformidad con el presente Acuerdo.

ARTÍCULO 20

Denuncia

1. Cualquiera de las Partes contratantes podrá denunciar el presente Acuerdo en cualquier momento mediante notificación escrita por vía diplomática, con un preaviso de tres meses.
2. Los datos personales incluidos en el ámbito de aplicación del presente Acuerdo y transferidos antes de la denuncia del presente Acuerdo seguirán siendo tratados de conformidad con el presente Acuerdo en el momento de la denuncia.
3. En caso de denuncia del presente Acuerdo, las Partes contratantes llegarán a un acuerdo sobre la continuación de la utilización y la conservación de la información ya comunicada entre ellas.

CAPÍTULO IV

DISPOSICIONES FINALES

ARTÍCULO 21

Relación con otros instrumentos internacionales

1. El presente Acuerdo no prejuzgará ni afectará de otro modo a las disposiciones jurídicas con respecto al intercambio de información previsto por cualquier tratado de asistencia judicial mutua, por cualquier otro acuerdo de cooperación o en las relaciones de trabajo en materia policial para el intercambio de información entre Nueva Zelanda y cualquier Estado miembro de la Unión.
2. El presente Acuerdo complementará el Acuerdo de trabajo por el que se establecen relaciones de cooperación entre la policía de Nueva Zelanda y la Agencia de la Unión Europea para la Cooperación Policial.

ARTÍCULO 22

Acuerdo administrativo de aplicación

Los pormenores de la cooperación entre las Partes contratantes correspondientes para la aplicación del presente Acuerdo serán objeto de un acuerdo administrativo de aplicación celebrado entre Europol y las autoridades competentes de Nueva Zelanda de conformidad con el Reglamento de Europol.

ARTÍCULO 23

Acuerdo administrativo sobre confidencialidad

Si es necesario en virtud del presente Acuerdo, el intercambio de información clasificada de la UE será regulado por un acuerdo administrativo sobre confidencialidad celebrado entre Europol y las autoridades competentes de Nueva Zelanda.

ARTÍCULO 24

Punto de contacto nacional y funcionarios de enlace

1. Nueva Zelanda designará un punto de contacto nacional que actuará como el punto de contacto central entre Europol y las autoridades competentes de Nueva Zelanda. Las tareas específicas del punto de contacto nacional se enumerarán en el acuerdo administrativo de aplicación a que se refiere el artículo 22. El punto de contacto nacional designado para Nueva Zelanda se indica en el anexo IV.
2. Europol y Nueva Zelanda reforzarán su cooperación tal y como se establece en el presente Acuerdo mediante el despliegue de uno o varios funcionarios de enlace por parte de Nueva Zelanda. Europol podrá enviar uno o varios funcionarios de enlace a Nueva Zelanda.

ARTÍCULO 25

Gastos

Las Partes contratantes garantizarán que las autoridades competentes sufraguen sus propios gastos derivados de la aplicación del presente Acuerdo, salvo disposición en contrario del mismo o del acuerdo administrativo de aplicación a que se refiere el artículo 22.

ARTÍCULO 26

Notificación de la aplicación

1. Cada Parte contratante dispondrá que las autoridades competentes pongan a disposición del público un documento en el que se expongan de forma inteligible las disposiciones relativas al tratamiento de los datos personales transferidos en virtud del presente Acuerdo, incluidos los medios disponibles para el ejercicio de los derechos de los interesados. Cada Parte contratante garantizará que se notifique una copia de dicho documento a la otra Parte contratante.
2. Cuando aún no se hayan establecido, las autoridades competentes adoptarán normas que especifiquen cómo se garantizará en la práctica el cumplimiento de las disposiciones relativas al tratamiento de datos personales transferidos en virtud del presente Acuerdo. Se notificará una copia de dichas normas a la otra Parte contratante y a las respectivas autoridades de control.

ARTÍCULO 27

Entrada en vigor y aplicación

1. El presente Acuerdo será aprobado por las Partes contratantes de conformidad con sus propios procedimientos.
2. El presente Acuerdo entrará en vigor en la fecha de recepción de la última notificación escrita en la que las Partes contratantes se hayan notificado mutuamente, por vía diplomática, que han concluido los procedimientos a que se refiere el apartado 1.
3. El presente Acuerdo será aplicable el primer día siguiente a la fecha en que se cumplan todas las condiciones siguientes:
 - a) el acuerdo administrativo de aplicación a que se refiere el artículo 22 ha pasado a ser aplicable;
 - b) las Partes contratantes se han notificado mutuamente que se han cumplido las obligaciones establecidas en el presente Acuerdo, incluidas las establecidas en el artículo 26, y dicha notificación ha sido aceptada.
4. Las Partes contratantes intercambiarán por vía diplomática notificaciones escritas que confirmen el cumplimiento de las condiciones mencionadas en el apartado 3.

ARTÍCULO 28

Modificaciones y suplementos

1. El presente Acuerdo podrá modificarse por escrito en cualquier momento, de común acuerdo entre las Partes contratantes, mediante notificación escrita intercambiada entre ellas por vía diplomática. Las modificaciones del presente Acuerdo entrarán en vigor con arreglo al procedimiento legal establecido en el artículo 27, apartados 1 y 2.
2. Los anexos del presente Acuerdo podrán actualizarse, cuando sea necesario, mediante el intercambio de notas diplomáticas. Dichas actualizaciones entrarán en vigor de conformidad con el procedimiento legal establecido en el artículo 27, apartados 1 y 2.
3. Las Partes contratantes iniciarán consultas sobre la modificación del presente Acuerdo o de sus anexos a petición una de las Partes contratantes.

ARTÍCULO 29

Revisión y evaluación

1. Las Partes contratantes revisarán conjuntamente la aplicación del presente Acuerdo un año después de su entrada en vigor y, posteriormente, a intervalos regulares y adicionalmente, a petición de cualquiera de las Partes contratantes y por decisión conjunta.
2. Las Partes contratantes evaluarán conjuntamente el presente Acuerdo cuatro años después de la fecha de su aplicación.

3. Las Partes contratantes decidirán por adelantado las modalidades de la revisión de la aplicación del presente Acuerdo y se comunicarán mutuamente la composición de sus respectivos equipos. Los equipos incluirán expertos pertinentes en los ámbitos de protección de datos y policial. Con sujeción a las disposiciones legales aplicables, todos los participantes en la revisión conjunta deberán respetar el carácter confidencial de los debates y contar con la correspondiente habilitación de seguridad. A efectos de cualquier revisión, la Unión y Nueva Zelanda garantizarán el acceso a la documentación, los sistemas y el personal pertinentes.

ARTÍCULO 30

Aplicación territorial

1. El presente Acuerdo se aplicará en el territorio en el que, y en la medida en que, sean aplicables el TUE y el TFUE, y en el territorio de Nueva Zelanda.
2. El presente Acuerdo solo se aplicará al territorio de Dinamarca si la Unión notifica por escrito a Nueva Zelanda que Dinamarca ha decidido quedar vinculada a este Acuerdo.
3. Si la Unión notifica a Nueva Zelanda antes de la fecha de entrada en vigor del presente Acuerdo que este se aplicará al territorio de Dinamarca, el presente Acuerdo se aplicará al territorio de Dinamarca el mismo día en que se aplique a los demás Estados miembros de la Unión.
4. Si la Unión notifica a Nueva Zelanda después de la entrada en vigor del presente Acuerdo que este se aplica al territorio de Dinamarca, el presente Acuerdo se aplicará al territorio de Dinamarca 30 días después de la fecha de dicha notificación.

ARTÍCULO 31

El presente Acuerdo se redacta en doble ejemplar, en lenguas alemana, búlgara, checa, croata, danesa, eslovaca, eslovena, española, estonia, finesa, francesa, griega, húngara, inglesa, irlandesa, italiana, letona, lituana, maltesa, neerlandesa, polaca, portuguesa, rumana y sueca, siendo cada uno de estos textos igualmente auténtico.

EN FE DE LO CUAL, los plenipotenciarios infrascritos, debidamente autorizados a tal fin, han firmado el presente Acuerdo.

Съставено в Брюксел на тридесети юни две хиляди двадесет и втора година.

Hecho en Bruselas, el treinta de junio de dos mil veintidós.

V Bruselu dne třicátého června dva tisíce dvacet dva.

Udfærdiget i Bruxelles den tredivte juni to tusind og toogtyve.

Geschehen zu Brüssel am dreißigsten Juni zweitausendzweiundzwanzig.

Kahe tuhande kahekümne teise aasta juunikuu kolmekümnendal päeval Brüsselis.

Έγινε στις Βρυξέλλες, στις τριάντα Ιουνίου δύο χιλιάδες είκοσι δύο.

Done at Brussels on the thirtieth day of June in the year two thousand and twenty two.

Fait à Bruxelles, le trente juin deux mille vingt-deux.

Arna dhéanamh sa Bhruiséil, an tríochadú lá de Mheitheamh sa bhliain dhá mhíle fiche agus a dó.

Sastavljeno u Bruxellesu tridesetog lipnja godine dvije tisuće dvadeset druge.

Fatto a Bruxelles, addì trenta giugno duemilaventidue.

Briselē, divi tūkstoši divdesmit otrā gada trīsdesmitajā jūnijā.

Priimta du tūkstančiai dvidešimt antrų metų birželio trisdešimtą dieną Briuselyje.

Kelt Brüsszelben, a kétezer-huszonkettedik év június havának harmincadik napján.

Magħmul fi Brussell, fit-tletin jum ta' Ġunju fis-sena elfejn u tnejn u għoxrin.

Gedaan te Brussel, dertig juni tweeduizend tweeëntwintig.

Sporządzono w Brukseli dnia trzydziestego czerwca roku dwa tysiące dwudziestego drugiego.

Feito em Bruxelas, em trinta de junho de dois mil e vinte e dois.

Întocmit la Bruxelles la treizeci iunie două mii douăzeci și doi.

V Bruseli tridsiateho júna dvetisícdvadsaťdva.

V Bruslju, tridesetega junija dva tisoč dvaindvajset.

Tehty Brysselissä kolmantenakymmenentenä päivänä kesäkuuta vuonna kaksituhattakaksikymmentäkaksi.

Som skedde i Bryssel den trettionde juni år tjugohundratjugotvå.

За Европейския съюз
 Por la Unión Europea
 Za Evropskou unii
 For Den Europæiske Union
 Für die Europäische Union
 Euroopa Liidu nimel
 Για την Ευρωπαϊκή Ένωση
 For the European Union
 Pour l'Union européenne
 Thar ceann an Aontais Eorpaigh
 Za Europejską uniję
 Per l'Unione europea
 Eiropas Savienības vārdā –
 Europos Sąjungos vardu
 Az Európai Unió részéről
 Ghall-Unjoni Ewropea
 Voor de Europese Unie
 W imieniu Unii Europejskiej
 Pela União Europeia
 Pentru Uniunea Europeană
 Za Európsku úniu
 Za Evropsko unijo
 Euroopan unionin puolesta
 För Europeiska unionen

peşe
 (Handwritten signature)

За Нова Зеландия
 Por Nueva Zelanda
 Za Nový Zéland
 For New Zealand
 Für Neuseeland
 Uus-Meremaa nimel
 Για τη Νέα Ζηλανδία
 For New Zealand
 Pour la Nouvelle-Zélande
 Thar ceann na Nua-Shéalainne
 Za Novi Zeland
 Per la Nuova Zelanda
 Jaunzēlandes vārdā –
 Naujosios Zelandijos vardu
 Új-Zéland részéről
 Għal New Zealand
 Voor Nieuw-Zeeland
 W imieniu Nowej Zelandii
 Pela Nova Zelândia
 Pentru Noua Zeelandă
 Za Nový Zéland
 Za Novo Zelandijo
 Uuden-Seelannin puolesta
 För Nya Zeeland

(Handwritten signature)

ANEXO I

ÁREAS DE DELINCUENCIA

Los delitos son:

- terrorismo,
- delincuencia organizada,
- narcotráfico,
- actividades de blanqueo de capitales,
- delitos relacionados con materiales nucleares o sustancias radiactivas,
- tráfico de inmigrantes,
- trata de seres humanos,
- delincuencia relacionada con vehículos de motor,
- homicidio voluntario, agresión con lesiones graves,
- tráfico ilícito de órganos y tejidos humanos,
- secuestro, detención ilegal y toma de rehenes,
- racismo y xenofobia,
- robo y hurto con agravantes,
- tráfico ilícito de bienes culturales, incluidas las antigüedades y obras de arte,
- estafa y fraude,
- delitos contra los intereses financieros de la Unión,
- operaciones con información privilegiada y manipulación del mercado financiero,
- chantaje y extorsión,
- falsificación y piratería,
- falsificación de documentos administrativos y tráfico de documentos administrativos falsos,
- falsificación de moneda y de medios de pago,
- ciberdelincuencia,
- corrupción,
- tráfico ilícito de armas, municiones y explosivos,
- tráfico ilícito de especies en peligro de extinción,
- tráfico ilícito de especies y variedades vegetales protegidas,
- delitos contra el medio ambiente, incluida la contaminación procedente de buques,
- tráfico ilícito de sustancias hormonales y otros factores de crecimiento,
- abusos sexuales y explotación sexual, incluido el material sobre abuso de menores y la captación de menores con fines sexuales,
- genocidio, crímenes contra la humanidad y crímenes de guerra.

Las formas de delincuencia a que se refiere el presente anexo serán evaluadas por las autoridades competentes de Nueva Zelanda de conformidad con la legislación de Nueva Zelanda.

*ANEXO II***AUTORIDADES COMPETENTES DE NUEVA ZELANDA Y SUS COMPETENCIAS**

Las autoridades competentes de Nueva Zelanda a las que Europol podrá transferir datos personales son las siguientes:

Policía de Nueva Zelanda (como autoridad competente principal de Nueva Zelanda)

Administración aduanera de Nueva Zelanda

Servicio de Inmigración de Nueva Zelanda

ANEXO III

LISTA DE ORGANISMOS DE LA UNIÓN

Misiones y operaciones de la Política Común de Seguridad y Defensa, limitadas a las actividades policiales

Oficina Europea de Lucha contra el Fraude (OLAF)

Agencia Europea de la Guardia de Fronteras y Costas (Frontex)

Banco Central Europeo (BCE)

Fiscalía Europea

Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust)

Oficina de Propiedad Intelectual de la Unión Europea (EUIPO)

ANEXO IV

PUNTO DE CONTACTO NACIONAL

El punto de contacto nacional central para que Nueva Zelanda actúe como punto de contacto central entre Europol y las autoridades competentes de Nueva Zelanda es:

Policía de Nueva Zelanda

Nueva Zelanda tiene la obligación de informar a Europol en caso de que cambie el punto de contacto nacional central de Nueva Zelanda.