REGLAMENTO (UE) 2019/818 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 20 de mayo de 2019

relativo al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración y por el que se modifican los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular, sus artículos 16, apartado 2; 74; 78, apartado 2, letra e); 79, apartado 2, letra c); 82, apartado 1, letra d); 85, apartado 1; 87, apartado 2, letra a), y 88, apartado 2,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo ([1]),

Previa consulta al Comité de las Regiones,

De conformidad con el procedimiento legislativo ordinario ([2]),

Considerando lo siguiente:

(1) En su Comunicación de 6 de abril de 2016 titulada «Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad», la Comisión subrayó la necesidad de mejorar la arquitectura de gestión de datos de la Unión para la gestión de las fronteras y la seguridad. La Comunicación puso en marcha un proceso destinado a lograr la interoperabilidad de los sistemas de información de la UE para la gestión de la seguridad, las fronteras y la migración, con el objetivo de solucionar las deficiencias estructurales relacionadas con estos sistemas que obstaculizan la labor de las autoridades nacionales y garantizar que los guardias de fronteras, las autoridades aduaneras, los agentes de policía y las autoridades judiciales tengan a su disposición la información necesaria.

(2) En su Hoja de ruta para mejorar el intercambio y la gestión de la información, con inclusión de soluciones de interoperabilidad en el ámbito de la Justicia y los Asuntos de Interior, de 6 de junio de 2016, el Consejo identificó varios retos jurídicos, técnicos y operativos para la interoperabilidad de los sistemas de información de la UE e instó a la búsqueda de soluciones.

(3) En su Resolución de 6 de julio de 2016 sobre las prioridades estratégicas para el programa de trabajo de la Comisión para 2017 ([3]), el Parlamento Europeo pidió que se presentaran propuestas para mejorar y desarrollar los sistemas de información de la UE existentes, colmar las lagunas de información y avanzar hacia su interoperabilidad, así como sus propuestas sobre la obligación de intercambiar información a nivel de la UE, junto con las salvaguardias necesarias en materia de protección de datos.

(4) En sus conclusiones de 15 de diciembre de 2016, el Consejo Europeo pidió continuidad en la obtención de resultados en materia de interoperabilidad de los sistemas de información y bases de datos de la UE.

(5) En su informe final de 11 de mayo de 2017, el Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad llegó a la conclusión de que es necesario y técnicamente viable trabajar para poner en marcha soluciones prácticas en materia de interoperabilidad y que la interoperabilidad podría, en principio, producir beneficios operativos y establecerse cumpliendo los requisitos sobre protección de datos.

(6) En su Comunicación de 16 de mayo de 2017 titulada «Séptimo informe de situación relativo a una Unión de la Seguridad genuina y efectiva», la Comisión diseñó, en consonancia con su Comunicación de 6 de abril de 2016 y las conclusiones y recomendaciones del Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad, un nuevo planteamiento para la gestión de los datos relativos a las fronteras, la seguridad y la migración, en virtud del cual todos los sistemas de información de la UE para la gestión de la seguridad, las fronteras y la migración serían interoperables sin menoscabo alguno de los derechos fundamentales.

([1]) DO C 283 de, 10.8.2018, p. 48.
([2]) Posición del Parlamento Europeo de 16 de abril de 2019 (pendiente de publicación en el Diario Oficial) y Decisión del Consejo de 14 de mayo de 2019.
([3]) DO C 101 de 16.3.2018, p. 116.

(7) En sus Conclusiones de 9 de junio de 2017 sobre los siguientes pasos para mejorar el intercambio de información y garantizar la interoperabilidad de los sistemas de información de la UE, el Consejo invitó a la Comisión a buscar soluciones de interoperabilidad según lo propuesto por el Grupo de Expertos de Alto Nivel.

(8) En sus conclusiones de 23 de junio de 2017, el Consejo Europeo puso de relieve la necesidad de mejorar la interoperabilidad de las bases de datos e invitó a la Comisión a preparar lo antes posible proyectos legislativos basados en las propuestas formuladas por el Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad.

(9) Con objeto de mejorar la efectividad y la eficiencia de los controles en las fronteras exteriores, contribuir a prevenir y combatir la inmigración ilegal y de alcanzar un elevado nivel de seguridad en el espacio de libertad, seguridad y justicia de la Unión, lo que incluye el mantenimiento de la seguridad pública y del orden público y la salvaguardia de la seguridad en el territorio de los Estados miembros, de mejorar la aplicación de la política común de visados y prestar asistencia en el examen de las solicitudes de protección internacional y en la prevención, detección e investigación de los delitos de terrorismo u otros delitos graves, ayudar a identificar a las personas desconocidas que no puedan identificarse o los restos humanos sin identificar en caso de catástrofes naturales, accidentes o atentados terroristas, con el fin de mantener la confianza de los ciudadanos en la política de migración y el sistema de asilo de la Unión, en las medidas de seguridad de la Unión y en las capacidades de la Unión en materia de gestión de las fronteras exteriores, debe establecerse la interoperabilidad de los sistemas de información de la UE, es decir el Sistema de Entradas y Salidas (SES), el Sistema de Información de Visados (VIS), el Sistema Europeo de Información y Autorización de Viajes (SEIAV), Eurodac, el Sistema de Información de Schengen (SIS), y el Sistema Europeo de Información de Antecedentes Penales de nacionales de terceros países (ECRIS-TCN), para que estos sistemas de información y sus datos se complementen mutuamente, respetando al mismo tiempo los derechos fundamentales de los individuos, especialmente el derecho a la protección de los datos personales. Para ello, deben crearse, como componentes de interoperabilidad, un portal europeo de búsqueda (PEB), un servicio de correspondencia biométrica compartido (SCB compartido), un registro común de datos de identidad (RCDI) y un detector de identidades múltiples (DIM).

(10) La interoperabilidad de los sistemas de información de la UE debe permitirles complementarse a fin de facilitar la identificación correcta de las personas, incluidas las personas desconocidas que no puedan identificarse o los restos humanos sin identificar, contribuir a luchar contra la usurpación de identidad, mejorar y armonizar los requisitos de calidad de los datos de los respectivos sistemas de información de la UE, facilitar la aplicación técnica y operativa por los Estados miembros de los sistemas de información de la UE, reforzar las garantías de seguridad de los datos y de protección de datos que rigen en los respectivos sistemas de información de la UE, racionalizar el acceso con fines de prevención, detección o investigación de los delitos de terrorismo u otros delitos graves al SES, el VIS, el SEIAV y Eurodac, y apoyar los objetivos del SES, el VIS, el SEIAV, Eurodac, el SIS y el ECRIS-TCN.

(11) Los componentes de interoperabilidad deben abarcar el SES, el VIS, el SEIAV, Eurodac, el SIS y el ECRIS-TCN. Asimismo deben incluir los datos de Europol, pero solo en la medida necesaria para que los datos de Europol puedan ser consultados al mismo tiempo que esos sistemas de información de la UE.

(12) Los componentes de interoperabilidad deben tratar los datos personales de personas cuyos datos personales sean tratados por los sistemas de información subyacentes de la UE y por Europol.

(13) Debe crearse un PEB con el fin de facilitar técnicamente a las autoridades de los Estados miembros y las agencias de la Unión Europea un acceso rápido, eficiente, sistemático y controlado los sistemas de información de la UE, los datos de Europol y las bases de datos de la Organización Internacional de Policía Criminal (Interpol) en la medida en que sea necesario para llevar a cabo sus tareas, de conformidad con sus derechos de acceso, así como para apoyar los objetivos del SES, el VIS, el SEIAV, Eurodac, el SIS, el ECRIS-TCN y los datos de Europol. Al permitir la consulta simultánea de todos los sistemas de información de la UE relevantes, en paralelo, así como de los datos de Europol y de las bases de datos de Interpol, el PEB debe actuar como una ventanilla única o «intermediario de mensajes» a distintos sistemas centrales de búsqueda y recabar la información necesaria de forma ininterrumpida y en el pleno respeto de las normas de control de acceso y los requisitos de protección de datos de los sistemas subyacentes.

(14) El diseño del PEB debe garantizar que, al iniciar una consulta de las bases de datos de Interpol, los datos utilizados por un usuario del PEB para iniciar una consulta de las bases de datos de Interpol no se compartan con los propietarios de los datos de Interpol. El diseño del PEB debe garantizar asimismo que las bases de datos de Interpol se consulten únicamente de conformidad con el Derecho nacional y de la Unión aplicable.

(15) Los usuarios del PEB que tengan derecho de acceso a los datos de Europol con arreglo al Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo ([4]) deben poder consultar simultáneamente los datos de Europol y los sistemas de información de la UE a los que tengan acceso. Cualquier otro tratamiento de datos que se derive de esa consulta debe tener lugar de conformidad con el Reglamento (UE) 2016/794, incluidas las limitaciones de acceso o de uso que imponga quien facilite los datos.

(16) El PEB debe desarrollarse y configurarse de tal forma que solo permita la utilización para las consultas utilizando datos que no sean relativos a personas o documentos de viaje que obren en un sistema de información de la UE, en los datos de Europol o en las bases de datos de Interpol.

(17) Para garantizar el uso sistemático de los sistemas de información de la UE pertinentes, el PEB debe utilizarse para consultar el RCDI, el SES, el VIS, el SEIAV, Eurodac y el ECRIS-TCN. Sin embargo, debe mantenerse la conexión nacional a los diferentes sistemas de información de la UE, a fin de proporcionar una alternativa técnica. Las agencias de la Unión también deben utilizar el PEB para consultar el SIS Central de conformidad con sus derechos de acceso, en el ejercicio de sus funciones. El PEB debe ser un medio suplementario para consultar el SIS Central, los datos de Europol y las bases de datos de Interpol, como complemento de las interfaces específicas existentes.

(18) Los datos biométricos, como las impresiones dactilares y las imágenes faciales, son únicos y, por tanto, mucho más fiables para la identificación de una persona que los datos alfanuméricos. El SCB compartido debe ser un instrumento técnico para reforzar y facilitar la labor de los sistemas de información de la UE relevantes y los demás componentes de interoperabilidad. El objetivo principal del SCB compartido debe ser facilitar la identificación de una persona que esté registrada en varias bases de datos, utilizando un único componente tecnológico para cotejar los datos biométricos de dicha persona entre diferentes sistemas, en lugar de varios componentes. El SCB compartido debe contribuir a la seguridad, así como aportar beneficios desde el punto de vista financiero, operativo y de mantenimiento. Todos los sistemas automáticos de identificación mediante impresiones dactilares, incluidos los utilizados actualmente para Eurodac, el VIS y el SIS, utilizan plantillas biométricas compuestas por los datos obtenidos mediante una extracción de características de muestras biométricas reales. El SCB compartido debe agrupar y almacenar todas estas plantillas biométricas —separadas de un modo lógico, según el sistema de información del que provengan los datos— en un único lugar, facilitando así el cotejo entre sistemas por medio de plantillas biométricas y permitir economías de escala en el desarrollo y el mantenimiento de los sistemas centrales de la UE.

(19) Las plantillas biométricas almacenadas en el SCB compartido deben estar formadas por datos procedentes de la extracción de características de las muestras biométricas reales y obtenerse de forma que no sea posible revertir el proceso de extracción. Las plantillas biométricas deben obtenerse a partir de datos biométricos, pero no debe ser posible obtener estos mismos datos biométricos a partir de las plantillas biométricas. Dado que los datos de las impresiones palmares y los perfiles de ADN solo se almacenan en el SIS y no pueden utilizarse para cotejarlos con los datos existentes en otros sistemas de información, en consonancia con los principios de necesidad y proporcionalidad, el SCB compartido no debe almacenar perfiles de ADN ni plantillas biométricas obtenidas a partir de datos de las impresiones palmares. deben estar formadas por datos procedentes de una extracción de características de las muestras biométricas reales y obtenerse de forma que no sea posible revertir el proceso de extracción. Las plantillas biométricas deben obtenerse a partir de datos biométricos, pero no debe ser posible obtener estos mismos datos biométricos a partir las plantillas biométricas. Dado que los datos de las impresiones palmares y los perfiles de ADN simplemente se almacenan en el SIS y no pueden utilizarse para cotejarlos con los datos existentes en otros sistemas de información, en consonancia con los principios de necesidad y proporcionalidad, el SCB compartido no debe almacenar perfiles de ADN ni plantillas biométricas obtenidas a partir de datos de las impresiones palmares.

(20) Los datos biométricos constituyen datos personales sensibles. El presente Reglamento debe establecer las bases y las salvaguardias para el tratamiento de dichos datos a los únicos efectos de la identificación inequívoca de las personas afectadas.

(21) El SES, el VIS, el SEIAV, Eurodac y el ECRIS-TCN necesitan una identificación exacta de las personas cuyos datos personales están almacenados en ellos. El RCDI debe, por consiguiente, facilitar la identificación correcta de las personas registradas en dichos sistemas.

(22) Los datos personales almacenados en los citados sistemas de información de la UE pueden referirse a las mismas personas, pero con identidades distintas o incompletas. Los Estados miembros disponen de métodos eficaces para identificar a sus ciudadanos o a los residentes permanentes registrados en su territorio. La interoperabilidad de los sistemas de información de la UE debe contribuir a la identificación correcta de las personas que figuran en esos sistemas. El RCDI debe almacenar aquellos datos personales que sean necesarios para permitir la identificación más precisa de las personas cuyos datos están almacenados en aquellos sistemas, incluida su identidad, los datos de su documento de viaje y sus datos biométricos, independientemente del sistema en el que se recogieran originalmente los datos. Solamente deben almacenarse en el RCDI los datos personales estrictamente necesarios para llevar a cabo un control de identidad adecuado. Los datos personales registrados en el RCDI no deben conservarse durante más tiempo del estrictamente necesario para los fines de los sistemas subyacentes y deben eliminarse automáticamente cuando se eliminen los datos en los sistemas subyacentes, con arreglo a su separación lógica.

([4]) 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).

(23) Es necesaria una nueva operación de tratamiento consistente en el almacenamiento de dichos datos en el RCDI, en lugar de su almacenamiento en cada uno de los diferentes sistemas, para mejorar la exactitud de la identificación mediante la comparación automatizada y las correspondencias entre dichos datos. El hecho de que los datos de identidad, del documento de viaje y los biométricos se almacenen en el RCDI no debe obstaculizar en modo alguno el tratamiento de datos para los fines de los Reglamentos del SES, el VIS, el SEIAV, Eurodac o el ECRIS-TCN, ya que el RCDI debe ser un nuevo componente compartido de dichos sistemas subyacentes.

(24) Es, por tanto, necesario crear un expediente individual en el RCDI para cada persona registrada en el SES, el VIS, el SEIAV, Eurodac o el ECRIS-TCN para alcanzar el objetivo de una identificación correcta de las personas dentro del espacio Schengen y para apoyar al MID, con la doble finalidad de facilitar los controles de identidad de los viajeros de buena fe y luchar contra la usurpación de identidad. El expediente individual debe almacenar en un único lugar toda la información de identidad vinculada a una persona, y dar acceso a ella a los usuarios finales debidamente autorizados.

(25) El RCDI debe, por lo tanto, facilitar y racionalizar el acceso de las autoridades responsables de la prevención, detección o investigación de delitos de terrorismo u otros delitos graves a los sistemas de información de la UE que no se hayan creado exclusivamente con fines de prevención, detección o investigación de delitos graves.

(26) El RCDI debe proporcionar un repositorio común de los datos de identidad, del documento de viaje y los biométricos de las personas registradas en el SES, el VIS, el SEIAV, Eurodac y el ECRIS-TCN. Debe ser parte de la arquitectura técnica de dichos sistemas y servir como componente compartido entre ellos para almacenar y consultar los datos de identidad, del documento de viaje y los biométricos que tratan.

(27) Todas las anotaciones del RCDI deben tener una separación lógica consistente en etiquetar automáticamente cada anotación con el nombre del sistema subyacente que lo contenga. El control de acceso del RCDI debe utilizar estas etiquetas para determinar si permite el acceso a la anotación en cuestión.

(28) Cuando las autoridades policiales de un Estado miembro no hayan podido identificar a una persona debido a la inexistencia de un documento de viaje u otro documento fiable que demuestre la identidad de esa persona, o cuando existan dudas sobre los datos de identidad proporcionados por esa persona o sobre la autenticidad del documento de viaje o la identidad de su titular, o cuando esa persona sea incapaz de cooperar o se niegue a hacerlo, dichas autoridades policiales deben poder consultar el RCDI al objeto de identificar a la persona. A tal fin, las autoridades policiales deben tomar las impresiones dactilares mediante técnicas de toma de impresiones dactilares en vivo y el procedimiento debe ser iniciado en presencia de dicha persona. Dichas consultas al RCDI no deben estar permitidas en los casos de identificación de menores de doce años, salvo que sea en el interés superior del menor.

(29) Cuando no puedan utilizarse los datos biométricos de la persona o si la consulta de esos datos es infructuosa, la consulta debe llevarse a cabo con los datos de identidad de dicha persona en combinación con los datos del documento de viaje. Cuando la consulta indique que los datos sobre la persona están almacenados en el RCDI, las autoridades de los Estados miembros deben tener acceso al RCDI para consultar los datos de identidad y los datos del documento de viaje de esa persona, sin que el RCDI proporcione ninguna indicación con respecto a qué sistema de información de la UE pertenecen los datos.

(30) Los Estados miembros deben adoptar medidas legislativas nacionales que designen a las autoridades competentes para llevar a cabo controles de identidad mediante el RCDI y establezcan los procedimientos, las condiciones y los criterios de dichos controles acordes con el principio de proporcionalidad. En particular, debe preverse en el Derecho nacional la facultad de recoger datos biométricos durante el control de identidad de una persona presente ante un miembro del personal de dichas autoridades.

(31) El presente Reglamento debe introducir también una nueva posibilidad de acceso racional a datos diferentes de los datos de identidad o los datos del documento de viaje registrados en el SES, el VIS, el SEIAV y Eurodac por parte de las autoridades responsables de la prevención, detección o investigación de los delitos de terrorismo u otros delitos graves designadas de los Estados miembros y de Europol. Estos datos pueden ser necesarios para la prevención, la detección o la investigación de delitos de terrorismo u otros delitos graves en un caso concreto, si existen motivos razonables para creer que su consulta contribuirá a la prevención, detección o investigación de los delitos de terrorismo u otros delitos graves en cuestión, en particular si existe una sospecha fundada de que el sospechoso, el autor o la víctima de un delito de terrorismo u otro delito grave es una persona cuyos datos están almacenados en el SES, el VIS, el SEIAV o Eurodac.

(32) El pleno acceso a los datos contenidos en los sistemas de información de la UE necesario para fines de prevención, detección o investigación de los delitos de terrorismo u otros delitos graves, más allá del acceso a los datos de identidad o a los datos del documento de viaje guardados en el RCDI debe seguir rigiéndose por los instrumentos jurídicos aplicables. Las autoridades responsables de la prevención, detección o investigación de los delitos de terrorismo u otros delitos graves designadas y Europol no saben de antemano cuáles de los sistemas de información de la UE contienen datos de las personas respecto de las cuales necesitan investigar. Esto da lugar a ineficiencias y retrasos. El usuario final autorizado por la autoridad designada debe, por lo tanto, estar autorizado a ver en cuál de los sistemas de información de la UE están registrados los datos que corresponden al resultado de su consulta. El sistema correspondiente, por tanto, se señalaría con una indicación tras la verificación automatizada de la presencia de una correspondencia en el sistema (la denominada funcionalidad de aviso de correspondencia).

(33) En este contexto, una respuesta del RCDI no debe interpretarse ni utilizarse como fundamento o razón para extraer conclusiones con respecto a una persona o tomar medidas contra ella, sino que solo debe utilizarse para presentar una solicitud de acceso a los sistemas de información subyacentes de la Unión, con arreglo a las condiciones y los procedimientos establecidos en los respectivos instrumentos jurídicos por los que se rige dicho acceso. Cualquier solicitud de acceso de este tipo debe estar sometida a las medidas previstas en el capítulo VII y, en su caso, a las medidas contempladas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([5]), en la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo ([6]) o en el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([7]).

(34) Como norma general, cuando un aviso de correspondencia indique que los datos están registrados en Eurodac, las autoridades designadas o Europol deben solicitar el pleno acceso al menos a uno de los sistemas de información de la UE de que se trate. En los casos en que, con carácter excepcional, no se solicite este pleno acceso, por ejemplo, porque las autoridades designadas o Europol ya han obtenido los datos por otros medios o porque la obtención de los datos ya no está permitida con arreglo al Derecho nacional, debe registrarse la justificación de la falta de solicitud de acceso.

(35) Los registros de las consultas del RCDI deben indicar la finalidad de la consulta. Cuando dicha consulta se haya llevado a cabo utilizando el planteamiento de consulta de datos en dos fases, los registros deben incluir una referencia al expediente nacional de la investigación o del caso, indicando de esta forma que dicha consulta ha sido iniciada con fines de prevención, detección o investigación de delitos de terrorismo u otros delitos graves.

(36) La consulta del RCDI por parte de las autoridades designadas y Europol para obtener un aviso de correspondencia que muestre que los datos están contenidos en el SES, el VIS, el SEIAV o Eurodac exige el tratamiento automatizado de datos personales. Un aviso de correspondencia no debe revelar datos personales de la persona de que se trate, aparte de la indicación de que algunos de sus datos están almacenados en uno de los sistemas. El usuario final autorizado no debe tomar ninguna decisión perjudicial para la persona de que se trate basándose únicamente en la presencia de un aviso de correspondencia. El acceso del usuario final a un aviso de correspondencia supondrá, por lo tanto, una interferencia muy limitada con el derecho a la protección de los datos personales de la persona de que se trate, al tiempo que permite a las autoridades designadas y a Europol solicitar el acceso a datos personales de forma más eficaz.

(37) Debe crearse un DIM para apoyar el funcionamiento del RCDI y de apoyar los objetivos del SES, el VIS, el SEIAV, Eurodac, el SIS y el ECRIS-TCN. Para ser eficaces en el cumplimiento de sus respectivos objetivos, todos los sistemas de información de la UE exigen la identificación exacta de las personas cuyos datos personales almacenan.

(38) Para mejorar la consecución de los objetivos de los sistemas de información de la UE, las autoridades que utilizan estos sistemas deben poder llevar a cabo verificaciones suficientemente fiables de las identidades de las personas cuyos datos estén almacenados en sistemas diferentes. El conjunto de datos de identidad o del documento de viaje

([5]) 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 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).

([6]) 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 (DO L 119 de 4.5.2016, p. 89).

([7]) Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39).

almacenados en un sistema individual concreto puede ser incorrecto, incompleto o fraudulento, y actualmente no existe ninguna posibilidad de detectar datos de identidad o del documento de viaje incorrectos, incompletos o fraudulentos por medio de una comparación con los datos almacenados en otro sistema. Para resolver esta situación, es necesario disponer de un instrumento técnico a escala de la Unión que permita la identificación correcta de las personas a esos efectos.

(39) El DIM debe crear y almacenar vínculos entre los datos de los distintos sistemas de información de la UE para detectar las identidades diferentes, con la doble finalidad de facilitar los controles de identidad de los viajeros de buena fe y de luchar contra la usurpación de identidad. Solamente debe contener los vínculos entre los datos de personas que figuran en más de un sistema de información de la UE. Los datos vinculados deben estar estrictamente limitados a aquellos datos que sean necesarios para verificar si una persona está registrada, ya sea de forma justificada o injustificada, con diferentes identidades biográficas en diferentes sistemas, o para aclarar que dos personas con similares datos biográficos pueden no ser la misma persona. El tratamiento de datos a través del PEB y del SCB compartido, destinado a vincular expedientes individuales entre diferentes sistemas individuales, debe quedar restringido a un mínimo absoluto y, por lo tanto, limitarse a la detección de identidades múltiples, que debe realizarse en el momento en que se añadan nuevos datos a uno de los sistemas que tengan datos almacenados en el RCDI o añadidos al SIS. El DIM debe incluir salvaguardias frente a una posible discriminación y decisiones desfavorables contra las personas con múltiples identidades legales.

(40) El presente Reglamento establece nuevas operaciones de tratamiento de datos destinadas a identificar correctamente a las personas de que se trate. Esto constituye una injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea. Dado que la aplicación eficaz de los sistemas de información de la UE depende de la identificación correcta de las personas afectadas, tal injerencia está justificada por los mismos objetivos para los que se ha creado cada uno de estos sistemas: la gestión eficaz de las fronteras de la Unión, la seguridad interna de la Unión y la aplicación efectiva de las políticas de la Unión en materia de visados y asilo.

(41) El PEB y el SCB compartido deben comparar los datos sobre personas contenidos en el RCDI y en el SIS cuando una autoridad nacional o una agencia de la UE creen o carguen nuevas anotaciones. Dicha comparación debe estar automatizada. El RCDI y el SIS deben utilizar el SCB compartido para detectar posibles vínculos basados en datos biométricos. El RCDI y el SIS deben utilizar el PEB para detectar posibles vínculos basados en datos alfanuméricos. El RCDI y el SIS deben poder identificar los mismos datos o datos similares relativos a una persona almacenados en varios sistemas. Cuando ese sea el caso, debe establecerse un vínculo que indique que se trata de la misma persona. El RCDI y el SIS deben configurarse de manera que detecten los pequeños errores de transliteración o de deletreo, a fin de que no sean fuentes de inconvenientes injustificados para la persona de que se trate.

(42) La autoridad nacional o la agencia de la UE que haya registrado los datos en el sistema de información de la UE respectivo debe confirmar o modificar esos vínculos. Esta autoridad nacional o agencia de la Unión debe tener acceso a los datos almacenados en el RCDI o el SIS y en el DIM, a efectos de la verificación manual de las diferentes identidades.

(43) La verificación manual de diferentes identidades debe ser garantizada por la autoridad que haya creado o actualizado los datos que hayan generado la correspondencia expresada mediante un vínculo con datos ya almacenados en otro sistema de información de la UE. La autoridad responsable de la verificación manual de identidades diferentes debe evaluar si existen múltiples identidades que se refieran a la misma persona de forma justificada o injustificada. Dicha evaluación debe llevarse a cabo, cuando sea posible, en presencia de la persona de que se trate y, en caso necesario, solicitando aclaraciones o información adicionales. La evaluación debe realizarse sin demora, de conformidad con los requisitos legales para la exactitud de la información que contemplen el Derecho nacional y de la Unión.

(44) Para los vínculos obtenidos en relación con las descripciones de personas buscadas para su detención, su entrega voluntaria o su extradición; personas desaparecidas o vulnerables; personas buscadas para que presten asistencia en un procedimiento judicial o personas buscadas a efectos de controles discretos, de controles de investigación o de controles específicos, la autoridad responsable de la verificación manual de las identidades diferentes debe ser la oficina Sirene del Estado miembro que haya creado la descripción. Dichas categorías de descripciones del SIS son sensibles y no deben necesariamente ser compartidas con las autoridades que hayan creado o actualizado

los datos vinculados a las mismas en uno de los otros sistemas de información de la UE. La creación de un vínculo con datos del SIS debe realizarse sin perjuicio de las medidas que deban adoptarse en virtud de los Reglamentos (UE) 2018/1860 ([8]), (UE) 2018/1861 ([9]) y (UE) 2018/1862 ([10]) del Parlamento Europeo y del Consejo.

(45) La creación de estos vínculos requiere transparencia en cuanto a las personas afectadas. Con el fin de facilitar la aplicación de las salvaguardias necesarias de conformidad con las normas de la Unión aplicables en materia de protección de datos, las personas que estén sujetas a un vínculo rojo o a un vínculo blanco a raíz de una verificación manual de identidades diferentes, deben ser informadas por escrito, sin perjuicio de las limitaciones para proteger la seguridad y el orden público, prevenir la delincuencia y garantizar que no se pongan en peligro las investigaciones nacionales. Estas personas deben recibir un número de identificación único que les permita identificar a la autoridad a la que deben dirigirse para ejercer sus derechos.

(46) Cuando exista un vínculo amarillo, la autoridad responsable de la verificación manual de las identidades diferentes debe tener acceso al RCD., Cuando exista un vínculo rojo, las autoridades de los Estados miembros y las agencias de la Unión que ya tengan acceso al menos a un sistema de información de la UE incluido en el RCDI o en el SIS deben tener acceso al DIM. Un vínculo rojo indica que una persona está utilizando diferentes identidades de manera injustificada, o que una persona está utilizando la identidad de otra persona.

(47) Cuando exista un vínculo blanco o verde entre datos procedentes de dos sistemas de información de la UE, las autoridades de los Estados miembros y las agencias de la Unión también deben tener acceso al DIM, si dichas autoridades o agencias tengan acceso a ambos sistemas de información. Dicho acceso debe concederse con el único fin de permitir que la autoridad o la agencia detecten casos en los que los datos puedan haber sido incorrectamente vinculados o tratados en el DIM, el RCDI y el SIS incumpliendo el presente Reglamento, así como para adoptar las medidas necesarias para corregir la situación y actualizar o suprimir el vínculo.

(48) La Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA) debe establecer mecanismos automatizados de control de calidad de los datos e indicadores comunes de calidad de los datos. Debe ser responsable de desarrollar una capacidad central de supervisión de la calidad de los datos y de elaborar informes periódicos de análisis de datos para mejorar el control de la implementación por los Estados miembros de los sistemas de información de la UE. Los indicadores comunes de calidad de los datos deben incluir las normas mínimas de calidad aplicables al almacenamiento de datos en los sistemas de información de la UE o en los componentes de interoperabilidad. El objetivo de dichas normas de calidad de los datos debe ser que los sistemas de información de la UE y los componentes de interoperabilidad identifiquen de forma automática presentaciones de datos aparentemente incorrectas o incoherentes, de modo que el Estado miembro que haya generado los datos pueda verificarlos y tomar las medidas correctoras que sean necesarias.

(49) La Comisión debe evaluar los informes de calidad de eu-LISA y formular recomendaciones a los Estados miembros cuando proceda. Los Estados miembros deben ser responsables de la preparación de un plan de acción que describa las medidas destinadas a corregir cualquier deficiencia en la calidad de los datos y deben informar periódicamente sobre sus progresos.

(50) El formato universal de mensajes (UMF) debe servir como norma para el intercambio de información, estructurado y transfronterizo, entre sistemas de información, autoridades u organizaciones en el ámbito de la justicia y los asuntos de interior. El UMF debe definir un vocabulario común y estructuras lógicas para la información intercambiada habitualmente con el objetivo de facilitar la interoperabilidad y permitir la creación y la lectura del contenido del intercambio de forma coherente y equivalente desde el punto de vista semántico.

(51) Puede tomarse en consideración la aplicación de la norma UMF en el VIS, el SIS y cualquier otro modelo existente o nuevo de intercambio transfronterizo de información o sistema de información en el ámbito de la justicia y los asuntos de interior desarrollado por los Estados miembros.

([8]) Reglamento (UE) 2018/1860 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, sobre la utilización del Sistema de Información de Schengen para el retorno de nacionales de terceros países en situación irregular (DO L 312 de 7.12.2018, p. 1).

([9]) Reglamento (UE) 2018/1861 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de las inspecciones fronterizas, por el que se modifica el Convenio de aplicación del Acuerdo de Schengen y se modifica y deroga el Reglamento (CE) n.º 1987/2006 (DO L 312 de 7.12.2018, p. 14).

([10]) Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y de la cooperación judicial en materia penal, por el que se modifica y deroga la Decisión 2007/533/JAI del Consejo, y se derogan el Reglamento (CE) n.º 1986/2006 del Parlamento Europeo y del Consejo y la Decisión 2010/261/UE de la Comisión (DO L 312 de 7.12.2018, p. 56).

(52) Debe crearse un repositorio central para la presentación de informes y estadísticas (RCIE), con el fin de generar datos estadísticos entre sistemas e informes de análisis relativos a la formulación de políticas, la operatividad y la calidad de los datos, de conformidad con los instrumentos jurídicos. eu-LISA debe crear e implementar el RCIE y alojarlo en sus sitios técnicos que contengan datos estadísticos anonimizados procedentes de los sistemas mencionados anteriormente, el RCDI, el DIM y el SCB compartido. Los datos contenidos en el RCIE no deben permitir la identificación de personas. eu-LISA debe anonimizar de forma automatizada los datos y registrar los datos anonimizados en el RCIE. El proceso para anonimizar los datos debe ser automatizado y no debe concederse al personal de eu-LISA acceso a ninguno de los datos personales almacenados en los sistemas de información de la UE o en los componentes de interoperabilidad.

(53) El Reglamento (UE) 2016/679 se aplica al tratamiento de datos personales con fines de interoperabilidad por parte de las autoridades nacionales en virtud del presente Reglamento, a menos que sean las autoridades designadas o los puntos de acceso central de los Estados miembros quienes lleven a cabo dicho tratamiento por razones de prevención, detección o investigación de los delitos de terrorismo u otros delitos graves.

(54) Cuando el tratamiento de los datos personales por parte de los Estados miembros con fines de interoperabilidad en virtud del presente Reglamento lo realicen las autoridades competentes a efectos de prevención, detección o investigación de los delitos de terrorismo o de otros delitos graves, debe ser de aplicación la Directiva (UE) 2016/680.

(55) El Reglamento (UE) 2016/679, el Reglamento (UE) 2018/1725 o, en su caso, la Directiva (UE) 2016/680, son aplicables a las transferencias de datos personales a terceros países u organizaciones internacionales realizadas de conformidad con el presente Reglamento. Sin perjuicio de los motivos de la transferencia con arreglo al capítulo V del Reglamento (UE) 2016/679 o, en su caso, de la Directiva (UE) 2016/680, toda resolución de un órgano jurisdiccional y toda decisión de una autoridad administrativa de un tercer país que exija a un responsable o encargado transferir o divulgar datos personales solo debe ser reconocida o ejecutable de alguna forma si se basa en un acuerdo internacional vigente entre el tercer país solicitante y la Unión o un Estado miembro.

(56) Las disposiciones específicas sobre protección de datos del Reglamento (UE) 2018/1862 y del Reglamento (UE) 2019/816 del Parlamento Europeo y del Consejo ([11]) son aplicables al tratamiento de datos personales en los sistemas regulados por esos Reglamentos.

(57) El Reglamento (UE) 2018/1725 es aplicable al tratamiento de los datos personales por eu-LISA y otras instituciones y organismos de la Unión en el ejercicio de sus responsabilidades con arreglo al presente Reglamento, sin perjuicio del Reglamento (UE) 2016/794, aplicable al tratamiento de datos personales por parte de Europol.

(58) Las autoridades de control a que se refiere el Reglamento (UE) 2016/679 o la Directiva (UE) 2016/680 deben supervisar la legalidad del tratamiento de los datos personales por los Estados miembros. El Supervisor Europeo de Protección de Datos debe supervisar las actividades que llevan a cabo las instituciones y organismos de la Unión en relación con el tratamiento de datos personales. El Supervisor Europeo de Protección de Datos y las autoridades de control deben cooperar en la supervisión del tratamiento de los datos personales que se realice mediante los componentes de interoperabilidad. Para que el Supervisor Europeo de Protección de Datos cumpla las tareas que le encomienda el presente Reglamento, se requieren recursos suficientes, tanto humanos como financieros.

(59) De conformidad con el artículo 28, apartado 2, del Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo ([12]), se consultó al Supervisor Europeo de Protección de Datos, que emitió su dictamen el 16 de abril de 2018 ([13]).

(60) El Grupo de Trabajo del Artículo 29 emitió un dictamen el 11 de abril de 2018.

(61) Los Estados miembros y eu-LISA deben disponer de planes de seguridad para facilitar el cumplimiento de las obligaciones en materia de seguridad y deben cooperar entre sí para solucionar los problemas de seguridad. eu-LISA también debe asegurarse de que se haga un uso continuo de los avances tecnológicos más recientes a fin de garantizar la integridad de los datos en el contexto del desarrollo, el diseño y la gestión de los componentes de

([11]) Reglamento (UE) 2019/816 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, por el que se establece un sistema centralizado para la identificación de los Estados miembros que poseen información sobre condenas de nacionales de terceros países y apátridas Penales (ECRIS-TCN) a fin de complementar el Sistema Europeo de Información de Antecedentes Penales, y por el que se modifica el Reglamento (UE) 2018/1726 (véase la página 1 del presente Diario Oficial).

([12]) Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1).

([13]) DO C 233 de 4.7.2018, p. 12.

interoperabilidad. Las obligaciones de eu-LISA a este respecto deben incluir la adopción de las medidas necesarias para impedir el acceso de personas no autorizadas, como el personal de proveedores de servicios externos, a datos personales tratados mediante los componentes de interoperabilidad. Al adjudicar contratos para la prestación de servicios, los Estados miembros y eu-LISA deben considerar todas las medidas necesarias para garantizar el cumplimiento de las disposiciones legislativas o reglamentarias relativas a la protección de los datos personales y la privacidad de las personas o salvaguardar intereses esenciales en materia de seguridad, de conformidad con el Reglamento (UE) 2018/1046 del Parlamento Europeo y del Consejo ([14]) y con los convenios internacionales aplicables. eu-LISA debe aplicar los principios de protección de la intimidad desde el diseño y por defecto durante el desarrollo de los componentes de interoperabilidad.

(62) Para apoyar los objetivos en materia de estadísticas e informes, es necesario conceder al personal autorizado de las autoridades, instituciones y agencias de la Unión competentes a que se refiere el presente Reglamento, acceso para consultar determinados datos relativos a determinados componentes de interoperabilidad sin permitir la identificación de las personas.

(63) A fin de permitir a las autoridades de los Estados miembros y las agencias de la Unión adaptarse a los nuevos requisitos sobre el uso del PEB, es necesario prever un periodo transitorio. Del mismo modo, a fin de garantizar la coherencia y el funcionamiento óptimo del DIM, deben adoptarse medidas transitorias para su entrada en funcionamiento.

(64) Dado que el objetivo del presente Reglamento, a saber, el establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE, no puede ser alcanzado de manera suficiente por los Estados miembros, sino que, debido a las dimensiones y a los efectos de la acción, puede lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea (TUE). De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

(65) El saldo asignado en el presupuesto a las fronteras inteligentes con arreglo al Reglamento (UE) n.º 515/2014 del Parlamento Europeo y del Consejo ([15]) debe reasignarse al presente Reglamento, de conformidad con el artículo 5, apartado 5, letra b), del Reglamento (UE) n.º 515/2014 al objeto de cubrir los costes del desarrollo de los componentes de interoperabilidad.

(66) A fin de complementar ciertos aspectos técnicos concretos del presente Reglamento, deben delegarse en la Comisión los poderes para adoptar actos con arreglo al artículo 290 del Tratado de Funcionamiento de la Unión Europea (TFUE), por lo que respecta a:

— la ampliación del período transitorio para el uso del PEB,

— la ampliación del período transitorio para la detección de identidad múltiple realizada por la unidad central del SEIAV,

— los procedimientos para determinar en qué casos puede considerarse que los datos de identidad son los mismos o similares,

— las normas de funcionamiento del RCIE, incluidas las salvaguardias específicas para el tratamiento de datos personales y las normas de seguridad aplicables al repositorio, y

— las normas detalladas sobre el funcionamiento del portal web.

Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos, y que esas consultas se realicen de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación ([16]). En particular, a fin de garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo deben recibir toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus expertos deben tener acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados.

(67) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución para para fijar las fechas a partir de las cuales deben comenzar a funcionar el PEB, el SCB compartido, el RCDI, el DIM y el RCIE.

([14]) Reglamento (UE, Euratom) 2018/1046 del Parlamento Europeo y del Consejo, de 18 de julio de 2018, sobre las normas financieras aplicables al presupuesto general de la Unión, por el que se modifican los Reglamentos (UE) n.º 1296/2013, (UE) n.º 1301/2013, (UE) n.º 1303/2013, (UE) n.º 1304/2013, (UE) n.º 1309/2013, (UE) n.º 1316/2013, (UE) n.º 223/2014 y (UE) n.º 283/2014 y la Decisión n.º 541/2014/UE y por el que se deroga el Reglamento (UE, Euratom) n.º 966/2012 (DO L 193 de 30.7.2018, p. 1).

([15]) Reglamento (UE) n.º 515/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, por el que se establece, como parte del Fondo de Seguridad Interior, el instrumento de apoyo financiero a las fronteras exteriores y los visados y por el que se deroga la Decisión 574/2007/CE (DO L 150 de 20.5.2014, p. 143).

([16]) DO L 123, de 12.5.2016, p. 1.

(68) También deben conferirse a la Comisión competencias de ejecución para adoptar normas detalladas relativas a: los detalles técnicos de los perfiles de los usuarios del PEB; las especificaciones de la solución técnica para facilitar la consulta de los sistemas de información de la UE, los datos de Europol y las bases de datos de Interpol por el PEB y el formato de las respuestas del PEB; las normas técnicas para la generación de vínculos entre datos de los distintos sistemas de información de la UE; el contenido y la presentación del formulario que se debe utilizar para informar al titular de los datos cuando se genere un vínculo rojo; los requisitos y la supervisión del rendimiento del SCB compartido; los mecanismos, procedimientos e indicadores del control automatizado de la calidad de los datos; el desarrollo de la norma UMF; el procedimiento de cooperación que se debe utilizar en caso de incidente de seguridad; y las especificaciones de la solución técnica para que los Estados miembros gestionen las solicitudes de acceso de los usuarios. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo ([17]).

(69) Ya que los componentes de interoperabilidad conllevarán el tratamiento de cantidades significativas de datos personales sensibles, es importante que las personas cuyos datos se traten a través de dichos componentes puedan ejercer de forma eficaz sus derechos como titulares de los datos, tal y como se dispone en el Reglamento (UE) 2016/679, la Directiva (UE) 2016/680 y el Reglamento (UE) 2018/1725. Los titulares de los datos deben disponer de un portal web que les facilite el ejercicio de sus derechos de acceso a sus datos personales y de rectificación, supresión y limitación del tratamiento de dichos datos. eu-LISA debe crear y gestionar dicho portal web.

(70) Uno de los principios fundamentales de la protección de datos es la minimización de datos: de conformidad con el artículo 5, apartado 1, letra c), del Reglamento (UE) 2016/679, que establece que el tratamiento de datos personales será adecuado, pertinente y limitado a lo necesario en relación con los fines para los que son tratados. Por esta razón, los componentes de interoperabilidad no deben prever el almacenamiento de nuevos datos personales, con excepción de los vínculos que se almacenarán en el DIM y que son el mínimo necesario a los efectos del presente Reglamento.

(71) El presente Reglamento debe contener disposiciones claras sobre responsabilidad civil y el derecho a una indemnización por daños y perjuicios causados por el tratamiento ilegal de datos personales y por cualquier otro acto incompatible con él. Las referidas disposiciones se entienden sin perjuicio del derecho a una indemnización y de la responsabilidad civil del responsable o del encargado del tratamiento en virtud del Reglamento (UE) 2016/679, la Directiva (UE) 2016/680 y el Reglamento (UE) 2018/1725. eu-LISA debe ser responsable, como encargada del tratamiento de datos, de los daños y perjuicios que cause cuando no cumpla las obligaciones que el presente Reglamento le impone específicamente, o cuando haya actuado al margen o en contra de las instrucciones legales del Estado miembro que sea responsable del tratamiento de los datos.

(72) El presente Reglamento se entiende sin perjuicio de la aplicación de la Directiva 2004/38/CE del Parlamento Europeo y del Consejo ([18]).

(73) De conformidad con los artículos 1 y 2 del Protocolo n.º 22 sobre la posición de Dinamarca, anejo al TUE y al TFUE, Dinamarca no participa en la adopción del presente Reglamento y no queda vinculada por este ni sujeta a su aplicación. Dado que el presente Reglamento, en la medida en que sus disposiciones se refieren al SIS según lo regulado por el Reglamento (UE) 2018/1862, desarrolla el acervo de Schengen, Dinamarca decidirá, de conformidad con el artículo 4 de dicho Protocolo, decidirá dentro de un período de seis meses a partir de que el Consejo haya tomado una medida sobre el presente Reglamento, si lo incorpora a su legislación nacional.

(74) En la medida en que sus disposiciones se refieren al SIS de conformidad con el Reglamento 2018/1862, el Reino Unido participa en este Reglamento, de conformidad con el artículo 5, apartado 1, del Protocolo n.º 19 sobre el acervo de Schengen integrado en el marco de la Unión Europea. anexo al TUE y al TFEU, y con el artículo 8, apartado 2, de la Decisión 2000/365/CE del Consejo ([19]). Además, en la medida en que sus disposiciones se relacionan con Eurodac y ECRIS-TCN, de conformidad con el artículo 3 del Protocolo n.º 21 sobre la posición del Reino Unido e Irlanda con respecto al espacio de libertad, seguridad y justicia, anexo al TUE y Al TFUE, el Reino Unido ha notificado, mediante carta de 18 de mayo de 2018, su deseo de participar en la adopción y aplicación del presente Reglamento.

([17]) Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).

([18]) Directiva 2004/38/CE del Parlamento Europeo y del Consejo, de 29 de abril de 2004, relativa al derecho de los ciudadanos de la Unión y de los miembros de sus familias a circular y residir libremente en el territorio de los Estados miembros, por la que se modifica el Reglamento (CEE) n.º 1612/68 y se derogan las Directivas 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE y 93/96/CEE (DO L 158 de 30.4.2004, p. 77).

([19]) Decisión 2000/365/CE del Consejo de 29 de mayo de 2000 sobre la solicitud del Reino Unido de Gran Bretaña e Irlanda del Norte de participar en algunas de las disposiciones del acervo de Schengen (DO L 131 de 1.6.2000, p. 43).

(75) En la medida en que las disposiciones del presente Reglamento se refieren al SIS según lo regulado por el Reglamento (UE) 2018/1862, Irlanda podría, en principio, participar en el presente Reglamento, de conformidad con el artículo 5, apartado 1, del Protocolo n.º19 del acervo Schengen integrado en el marco de la Unión Europea, anejo al TUE y al TFUE, y al artículo 6, apartado 2, de la Decisión 2002/192/ CE del Consejo ([20]). Además, en la medida en las disposiciones del presente Reglamento se refieren a Eurodac y el ECRIS-TCN, de conformidad con los artículos 1 y 2 y del Protocolo n.º 21 sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia, adjunto al TUE y al TFUE, y sin perjuicio del artículo 4 de dicho Protocolo, Irlanda no participa en la adopción del presente Reglamento y no queda vinculada por él ni sujeta a su aplicación. Dado que no es posible, en estas circunstancias, garantizar que el presente Reglamento sea aplicable en su totalidad a Irlanda, como lo exige el artículo 288 del TFUE, Irlanda no participa en la adopción del presente Reglamento y no queda vinculada por él ni sujeta a su aplicación, sin perjuicio de sus derechos en virtud de los Protocolos n.º 19 y n.º 21.

(76) . Por lo que respecta a Islandia y Noruega, el presente Reglamento constituye, en la medida en que se refiere al SIS según lo regulado por el Reglamento 2018/1862, un desarrollo de las disposiciones del acervo de Schengen en el sentido del Acuerdo celebrado por el Consejo de la Unión Europea y la República. de Islandia y el Reino de Noruega sobre la asociación de estos dos Estados a la ejecución, aplicación y desarrollo del acervo de Schengen, ([21]) que se entran dentro del ámbito mencionado en el artículo 1, punto G, de la Decisión 1999/437/CE del Consejo ([22]).

(77) . Por lo que respecta a Suiza, el presente Reglamento constituye, en la medida en que se refiere al SIS según lo regulado por el Reglamento (UE) 2018/1862, un desarrollo de las disposiciones del acervo de Schengen en el sentido del Acuerdo celebrado entre la Unión Europea, la Comunidad Europea y la Confederación Suiza sobre la asociación de la Confederación Suiza a la ejecución, aplicación y desarrollo del acervo de Schengen ([23]) que entran dentro del ámbito mencionado en el artículo 1, punto G, de la Decisión 1999/437/CE del Consejo en relación con el artículo 3 de la Decisión 2008/149/JAI del Consejo ([24]).

(78) Por lo que respecta a Liechtenstein, el presente Reglamento constituye, en la medida en que se refiere al SIS según lo regulado por el Reglamento (UE) 2018/1862, un desarrollo de las disposiciones del acervo de Schengen en el sentido del Acuerdo celebrado entre la Unión Europea, la Comunidad Europea, la Confederación Suiza y el Principado de Liechtenstein referente a la adhesión del Principado de Liechtenstein al Acuerdo entre la Unión Europea, la Comunidad Europea y la Confederación Suiza a la asociación de la Confederación Suiza a la ejecución, aplicación y desarrollo del acervo de Schengen ([25]) que entran en el ámbito mencionado en el artículo 1, punto G, de la Decisión 1999/437/CE, en relación con el artículo 3 de la Decisión 2011/350/UE del Consejo ([26]).

(79) El presente Reglamento respeta los derechos fundamentales y observa los principios reconocidos, en particular, en la Carta de los Derechos Fundamentales de la Unión Europea, por lo que debe aplicarse de conformidad con tales derechos y principios.

(80) A fin de que el presente Reglamento encaje en el marco jurídico vigente, el Reglamento (UE) 2018/1726 del Parlamento Europeo y del Consejo ([27]) y los Reglamentos (UE) 2018/1862 y (UE) 2019/816 deben modificarse en consecuencia.

([20]) Decisión 2002/192/CE del Consejo, de 28 de febrero de 2002, sobre la solicitud de Irlanda de participar en algunas de las disposiciones del acervo de Schengen (DO L 64 de 7.3.2002, p. 20).

([21]) DO L 176 de 10.7.1999, p. 36.

([22]) Decisión 1999/437/CE del Consejo, de 17 de mayo de 1999, relativa a determinadas normas de desarrollo del Acuerdo celebrado por el Consejo de la Unión Europea con la República de Islandia y el Reino de Noruega sobre la asociación de estos dos Estados a la ejecución, aplicación y desarrollo del Acervo de Schengen (DO L 176 de 10.7.1999, p. 31).

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

([24]) Decisión 2008/149/JAI del Consejo, de 28 de enero de 2008, relativa a la celebración, en nombre de la Unión Europea, del Acuerdo entre la Unión Europea, la Comunidad Europea y la Confederación Suiza sobre la asociación de la Confederación Suiza a la ejecución, aplicación y desarrollo del acervo de Schengen (DO L 53 de 27.2.2008, p. 50).

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

([26]) Decisión 2011/350/UE del Consejo, de 7 de marzo de 2011, relativa a la celebración, en nombre de la Unión Europea, del Protocolo entre la Unión Europea, la Comunidad Europea, la Confederación Suiza y el Principado de Liechtenstein sobre la adhesión del Principado de Liechtenstein al Acuerdo entre la Unión Europea, la Comunidad Europea y la Confederación Suiza sobre la asociación de la Confederación Suiza a la ejecución, aplicación y desarrollo del acervo de Schengen, sobre la supresión de controles en las fronteras internas y la circulación de personas (DO L 160 de 18.6.2011, p. 19).

([27]) Reglamento (UE) 2018/1726 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a la Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA), y por el que se modifican el Reglamento (CE) n.º 1987/2006 y la Decisión 2007/533/JAI del Consejo y se deroga el Reglamento (UE) n.º 1077/2011 (DO L 295 de 21.11.2018, p. 99).

HAN ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I

Disposiciones generales

Artículo 1

Objeto

1. El presente Reglamento, junto con el Reglamento (UE) 2019/817 del Parlamento Europeo y del Consejo ([28]), establece un marco para garantizar la interoperabilidad del Sistema de Entradas y Salidas (SES), el Sistema de Información de Visados (VIS), el Sistema Europeo de Información y Autorización de Viajes (SEIAV), Eurodac, el Sistema de Información de Schengen (SIS) y el Sistema Europeo de Información de Antecedentes Penales de nacionales de terceros países (ECRIS-TCN).

2. El marco incluirá los siguientes componentes de interoperabilidad:

a) un portal europeo de búsqueda (PEB);

b) un servicio de correspondencia biométrica compartido (SCB compartido);

c) un registro común de datos de identidad (RCDI);

d) un detector de identidades múltiples (DIM).

3. El presente Reglamento establece también disposiciones sobre los requisitos de calidad de los datos, sobre un formato universal de mensajes (UMF) y sobre un repositorio central de presentación de informes y estadísticas (RCIE), además de las responsabilidades de los Estados miembros y de la Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA), en lo que respecta al diseño, el desarrollo y el funcionamiento de los componentes de interoperabilidad.

4. El presente Reglamento también adapta los procedimientos y condiciones para el acceso de las autoridades designadas y de la Agencia de la Unión Europea para la Cooperación Policial (Europol) al SES, al VIS, al SEIAV y a Eurodac con fines de prevención, detección o investigación de los delitos de terrorismo u otros delitos graves.

5. El presente Reglamento establece asimismo un marco para la verificación manual de la identidad de las personas y para la identificación de las personas.

Artículo 2

Objetivos

1. Mediante la garantía de la interoperabilidad, el presente Reglamento tiene los siguientes objetivos:

a) mejorar la efectividad y la eficiencia de las inspecciones fronterizas en las fronteras exteriores;

b) contribuir a la prevención de la inmigración ilegal y a la lucha contra ella;

c) contribuir a un alto nivel de seguridad en el espacio de libertad, seguridad y justicia de la Unión, lo que incluye el mantenimiento de la seguridad pública y del orden público y la salvaguardia de la seguridad en el territorio de los Estados miembros;

d) mejorar la aplicación de la política común de visados;

e) ayudar a examinar las solicitudes de protección internacional;

f) contribuir a la prevención, detección e investigación de los delitos de terrorismo o de otros delitos penales graves;

g) ayudar a identificar a las personas desconocidas que no puedan identificarse o los restos humanos sin identificar en caso de catástrofes naturales, accidentes o atentados terroristas.

2. Los objetivos contemplados en el apartado 1 se alcanzarán:

a) garantizando la identificación correcta de las personas;

b) contribuyendo a luchar contra la usurpación de identidad;

([28]) Reglamento (UE) 2019/817 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de las fronteras y los visados y por el que se modifican los Reglamentos (CE) n.º 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 y (UE) 2018/1861 del Parlamento Europeo y del Consejo, y las Decisiones 2004/512/CE y 2008/633/JAI del Consejo (véase la página 27 del presente Diario Oficial).

c) mejorando la calidad de los datos y armonizando los requisitos de calidad de los datos almacenados en los sistemas de información de la UE, respetando al mismo tiempo los requisitos de tratamiento de datos de los instrumentos jurídicos que rigen los diferentes sistemas y las normas y principios en materia de protección de datos;

d) facilitando y apoyando la aplicación técnica y operativa por parte de los Estados miembros de los sistemas de información de la UE;

e) reforzando, simplificando y uniformizando las condiciones de seguridad de los datos y de protección de datos que rigen en los respectivos sistemas de información de la UE, sin perjuicio de la protección y las salvaguardias especiales otorgadas a ciertas categorías de datos;

f) racionalizando las condiciones de acceso de las autoridades designadas al SES, al VIS, al SEIAV y a Eurodac, garantizando al mismo tiempo las condiciones necesarias y proporcionadas para dicho acceso;

g) apoyando los objetivos del SES, el VIS, el SEIAV, Eurodac, el SIS y el ECRIS-TCN.

Artículo 3

Ámbito de aplicación

1. El presente Reglamento es aplicable a Eurodac, al SIS y al ECRIS-TCN.

2. El presente Reglamento también es aplicable a los datos de Europol, en la medida de permitir consultarlos de manera simultánea con los sistemas de información de la UE a que se refiere el apartado 1.

3. El presente Reglamento es aplicable a las personas cuyos datos personales puedan ser objeto de tratamiento en los sistemas de información de la UE a que se refiere el apartado 1 y en los datos de Europol a que se refiere el apartado 2.

Artículo 4

Definiciones

A los efectos del presente Reglamento, se entenderá por:

1) «fronteras exteriores»: las fronteras exteriores tal como se definen en el artículo 2, punto 2), del Reglamento (UE) 2016/399 del Parlamento Europeo y del Consejo ([29]);

2) «inspecciones fronterizas»: las inspecciones fronterizas tal como se definen en el artículo 2, punto 11, del Reglamento (UE) 2016/399;

3) «autoridad fronteriza»: la guardia de fronteras encargada de llevar a cabo las inspecciones fronterizas de conformidad con la normativa nacional;

4) «autoridades de control»: las autoridades de control a que se refiere el artículo 51, apartado 1, del Reglamento (UE) 2016/679 y las autoridades de control a que se refiere el artículo 41, apartado 1, punto 1, de la Directiva (UE) 2016/680;

5) «verificación»: el proceso de comparación de conjuntos de datos para establecer la validez de una identidad declarada (control simple);

6) «identificación»: el proceso de determinación de la identidad de una persona por comparación con múltiples conjuntos de datos de una base de datos (control múltiple);

7) «datos alfanuméricos»: datos representados por letras, dígitos, caracteres especiales, espacios y signos de puntuación;

8) «datos de identidad»: los datos a que se refiere el artículo 27, apartado 3, letras a) a e);

9) «datos dactiloscópicos»: imágenes de las impresiones dactilares e imágenes de impresiones dactilares latentes que, debido a su carácter único y a los puntos de referencia que contienen, permiten comparaciones concluyentes y precisas sobre la identidad de una persona;

([29]) Reglamento (UE) 2016/399 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, por el que se establece un Código de normas de la Unión para el cruce de personas por las fronteras (Código de fronteras Schengen) (DO L 77 de 23.3.2016, p. 1).

10) «imagen facial»: las imágenes digitales del rostro de una persona;

11) «datos biométricos»: los datos dactiloscópicos las imágenes faciales;

12) «plantilla biométrica»: una representación matemática obtenida por extracción de características de los datos biométricos, limitada a las características necesarias para llevar a cabo identificaciones y verificaciones;

13) «documento de viaje»: el pasaporte o cualquier otro documento equivalente que permita a su titular cruzar las fronteras exteriores y en el que pueda insertarse el visado;

14) «datos del documento de viaje»: el tipo, el número y el país de expedición del documento de viaje, la fecha de expiración de su validez y el código de tres letras del país de expedición;

15) «sistemas de información de la UE»: el SES, el VIS, el SEIAV, Eurodac, el SIS y el ECRIS-TCN;

16) «datos de Europol»: los datos personales tratados por Europol a efectos del artículo 18, apartado 2, letras a), b) y c), del Reglamento (UE) 2016/794;

17) «bases de datos de Interpol»: la base de datos sobre documentos de viaje robados y perdidos (base de datos DVRP) de Interpol y la base de datos de documentos de viaje asociados a notificaciones de Interpol (base de datos TDAWN);

18) «correspondencia»: la existencia de una coincidencia como resultado de una comparación automatizada entre datos personales que hayan sido o estén siendo registrados en un sistema de información o una base de datos;

19) «autoridades policiales»: las «autoridades competentes» tal como se definen en el artículo 3, punto 7), de la Directiva (UE) 2016/680;

20) «autoridades designadas»: las autoridades designadas por el Estado miembro tal como se definen en el artículo 3, apartado 1, punto 26, del Reglamento (UE) 2017/2226 del Parlamento Europeo y del Consejo ([30]), el artículo 2, apartado 1, letra e), de la Decisión 2008/633/JAI del Consejo ([31]), y el artículo 3, apartado 1, punto 21, del Reglamento (UE) 2018/1240 del Parlamento Europeo y el Consejo ([32]);

21) «delito de terrorismo»: un delito con arreglo a al Derecho nacional que corresponda o sea equivalente a alguno de los delitos a que se refiere la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo ([33]);

22) «delito grave»: un delito que corresponda o sea equivalente a alguno de los delitos a los que se refiere el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI del Consejo ([34]), si está penado en el Derecho nacional con una pena privativa de libertad o de internamiento con una duración máxima no inferior a tres años;

23) «Sistema de Entradas y Salidas ("SES")»: el Sistema de Entradas y Salidas establecido en el Reglamento (UE) 2017/2226;

24) «Sistema de Información de Visados ("VIS")»: el Sistema de Información de Visados a que se refiere el Reglamento (CE) n.º 767/2008 del Parlamento Europeo y del Consejo ([35]);

25) «Sistema Europeo de Información y Autorización de Viajes ("SEIAV")»: el Sistema Europeo de Información y Autorización de Viajes establecido en el Reglamento (UE) 2018/1240;

([30]) Reglamento (UE) 2017/2226 del Parlamento Europeo y el Consejo, de 30 de noviembre de 2017, por el que se establece un Sistema de Entradas y Salidas (SES) para registrar los datos de entrada y salida y de denegación de entrada relativos a nacionales de terceros países que crucen las fronteras exteriores de los Estados miembros, se determinan las condiciones de acceso al SES con fines policiales y se modifican el Convenio de aplicación del Acuerdo de Schengen y los Reglamentos (CE) n.º 767/2008 y (UE) n.º 1077/2011 (Reglamento SES) (DO L 327 de 9.12.2017, p. 20).

([31]) Decisión 2008/633/JAI del Consejo, de 23 de junio de 2008, sobre el acceso para consultar el Sistema de Información de Visados (VIS) por las autoridades designadas de los Estados miembros y por Europol, con fines de prevención, detección e investigación de delitos de terrorismo y otros delitos graves (Decisión 2008/633/JAI del Consejo, de 23 de junio de 2008, sobre el acceso para consultar el Sistema de Información de Visados (VIS) por las autoridades designadas de los Estados miembros y por Europol, con fines de prevención, detección e investigación de delitos de terrorismo y otros delitos graves (DO L 218 de 13.8.2008, p. 129).

([32]) Reglamento (UE) 2018/1240 del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, por el que se establece un Sistema Europeo de Información y Autorización de Viajes (SEIAV) y por el que se modifican los Reglamentos (UE) n.º 1077/2011, (UE) n.º 515/2014, (UE) 2016/399, (UE) 2016/1624 y (UE) 2017/2226 (DO L 236 de 19.9.2018, p. 1).

([33]) Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión Marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo (DO L 88 de 31.3.2017, p. 6).

([34]) Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros (DO L 190 de 18.7.2002, p. 1).

([35]) Reglamento CE n.º 767/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (Reglamento VIS) (DO L 218 de 13.8.2008, p. 60).

26) «Eurodac»: Eurodac establecido por el Reglamento (UE) n.º 603/2013 del Parlamento Europeo y del Consejo ([36]);

27) «Sistema de Información de Schengen ("SIS")»: el Sistema de Información de Schengen a que se refieren los Reglamentos (UE) 2018/1860, (UE) 2018/1861, y (UE) 2018/1862;

28) «ECRIS-TCN»: el sistema centralizado para la identificación de los Estados miembros que contiene información sobre las condenas de nacionales de terceros países y apátridas establecido en el Reglamento (UE) 2019/816.

Artículo 5

No discriminación y derechos fundamentales

El tratamiento de datos personales a los efectos del presente Reglamento no dará lugar a discriminación contra las personas por motivos tales como el género, la raza, el color, el origen étnico o social, las características genéticas, el idioma, la religión o las creencias, las opiniones políticas o de cualquier otro tipo, la pertenencia a una minoría nacional, el patrimonio, el nacimiento, la discapacidad, la edad o la orientación sexual. Deberá respetar plenamente la dignidad y la integridad humanas, así como los derechos fundamentales, incluido el derecho a la intimidad y a la protección de los datos personales. Se prestará especial atención a los niños, las personas mayores, las personas con discapacidad y las personas que necesitan protección internacional. El interés superior del menor constituirá una consideración primordial.

CAPÍTULO II

Portal europeo de búsqueda

Artículo 6

Portal europeo de búsqueda

1. Se crea un Portal europeo de búsqueda (PEB) con objeto de facilitar el acceso en casos rápido, ininterrumpido, sistemático y controlado de las autoridades de los Estados miembros y de las agencias de la Unión a los sistemas de información de la UE, a los datos de Europol y las bases de datos de Interpol para el desempeño de sus tareas y de conformidad con sus derechos de acceso, así como con los objetivos y fines del SES, VIS, SEIAV, Eurodac, el SIS y ECRIS-TCN.

2. El PEB se compondrá de:

a) una infraestructura central, incluido un portal de búsqueda que permita la consulta simultánea del SES, el VIS, el SEIAV, el SIS, Eurodac y el ECRIS-TCN, así como de los datos de Europol y las bases de datos de Interpol;

b) un canal de comunicación seguro entre el PEB, los Estados miembros y las agencias de la Unión que tengan derecho a utilizar el PEB;

c) una infraestructura de comunicación segura entre el PEB y el SES, el VIS, el SEIAV Eurodac, el SIS Central, el ECRIS-TCN, los datos de Europol y las bases de datos de Interpol, así como entre el PEB y las infraestructuras centrales del RCDI y el DIM.

3. eu-LISA desarrollará el PEB y garantizará su gestión técnica.

Artículo 7

Utilización del portal europeo de búsqueda

1. La utilización del PEB se reservará a las autoridades de los Estados miembros y a las agencias de la Unión que tengan acceso como mínimo a uno de los sistemas de información de la UE, de conformidad con los instrumentos jurídicos que rijan esos sistemas, al RCDI y al DIM de conformidad con el presente Reglamento, a los datos de Europol de conformidad con el Reglamento (UE) 2016/794 o a las bases de datos de Interpol de conformidad con el Derecho nacional o de la Unión que regule dicho acceso.

Dichas autoridades de los Estados miembros y agencias de la Unión podrán utilizar el PEB y los datos que este facilite únicamente para los objetivos y fines establecidos en los instrumentos jurídicos que rigen dichos sistemas de información de la UE, en el Reglamento (UE) 2016/794 y en el presente Reglamento.

([36]) Reglamento (UE) n.º 603/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (UE) n.º 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley, y por el que se modifica el Reglamento (UE) n.º1 1077/2011, por el que se crea una Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia (DO L 180 de 29.6.2013, p. 1).

2. Las autoridades de los Estados miembros y de las agencias de la Unión a que se refiere el apartado 1 utilizarán el PEB para consultar datos relativos a personas o sus documentos de viaje en los sistemas centrales de Eurodac y el ECRIS-TCN de conformidad con sus derechos de acceso a que se refieren los instrumentos jurídicos que rigen los sistemas de información de la UE y en el Derecho nacional. Asimismo, utilizarán el PEB para consultar el RCDI, de conformidad con sus derechos de acceso con arreglo al presente Reglamento, para los fines mencionados en los artículos 20, 21 y 22.

3. Las autoridades de los Estados miembros a que se refiere el apartado 1 pueden utilizar el PEB para buscar datos relativos a las personas o sus documentos de viaje en el SIS Central a que se refieren los Reglamentos (UE) 2018/1860 y (UE) 2018/1861.

4. Cuando así se estipule en el Derecho de la Unión, las agencias de la Unión mencionadas en el apartado 1 utilizarán el PEB para consultar datos relativos a personas o sus documentos de viaje en el SIS Central.

5. Las autoridades a que se refiere el apartado 1 utilizarán el PEB para consultar datos relativos a personas o sus documentos de viaje en los datos de Europol, de conformidad con los derechos de acceso que les otorguen el Derecho de la Unión y nacional.

Artículo 8

Perfiles de los usuarios del portal europeo de búsqueda

1. A los efectos de permitir el uso del PEB, eu-LISA creará, en colaboración con los Estados miembros, un perfil basado en la categoría de usuarios del PEB y en el objeto de sus consultas, de conformidad con los detalles técnicos y derechos de acceso a que se refiere el apartado 2. Cada perfil incluirá, de conformidad con el Derecho de la Unión y nacional, la información siguiente:

a) los campos de datos que tienen que utilizarse para llevar a cabo una consulta;

b) los sistemas de información de la UE, los datos de Europol y las bases de datos de Interpol que tienen que consultarse, cuáles pueden consultarse y cuales tienen que dar una respuesta al usuario;

c) los datos específicos en los sistemas de información de la UE, los datos de Europol y las bases de datos de Interpol que pueden consultarse;

d) las categorías de datos que pueden facilitarse en cada respuesta.

2. La Comisión adoptará actos de ejecución para especificar los detalles técnicos de los perfiles a que se refiere el apartado 1, de conformidad con los derechos de acceso de los usuarios del PEB, en virtud de los instrumentos jurídicos que rigen los sistemas de información de la UE y en el Derecho nacional. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 70, apartado 2.

3. Los perfiles a que se refiere el apartado 1 serán revisados periódicamente por eu-LISA en colaboración con los Estados miembros, al menos una vez al año, y, cuando proceda, se actualizarán.

Artículo 9

Consultas

1. Los usuarios del PEB iniciarán una consulta mediante la presentación de datos alfanuméricos y/o biométricos al PEB. Cuando se haya iniciado una consulta, el PEB consultará el SES, el SEIAV, el VIS, el SIS, Eurodac, el ECRIS-TCN, el RCDI, los datos de Europol y las bases de datos de Interpol al mismo tiempo que los datos presentados por el usuario y de conformidad con el perfil de este.

2. Las categorías de datos utilizados para iniciar una consulta a través del PEB corresponderán a las categorías de datos relacionados con personas o documentos de viaje que puedan utilizarse para consultar los distintos sistemas de información de la UE, los datos de Europol y las bases de datos de Interpol, de conformidad con los instrumentos jurídicos que los rijan.

3. eu-LISA, en colaboración con los Estados miembros, desarrollará un documento de control de interfaces sobre la base del UMF a que se refiere el artículo 38 para el PEB.

4. Cuando se lance una consulta por un usuario del PEB, el SES, el SEIAV, el VIS, el SIS, Eurodac, el ECRIS-TCN, el RCDI y el DIM, así como los datos de Europol y las bases de datos de Interpol, proporcionarán como respuesta a la consulta los datos oportunos contenidos en ellas.

Sin perjuicio de el artículo 20, la respuesta facilitada por el PEB indicará a qué sistema de información de la UE o base de datos pertenecen los datos.

El PEB no facilitará información relativa a los datos almacenados en sistemas de información de la UE, los datos de Europol y las bases de datos de Interpol a los que el usuario no tenga acceso con arreglo a el Derecho de la Unión y nacional aplicable.

5. Toda consulta de las bases de datos de Interpol, iniciada a través del PEB se realizará de tal manera que no se revele ningún elemento de dicha información al propietario de la descripción Interpol.

6. El PEB dará respuestas al usuario tan pronto como se disponga de datos procedentes de uno de los sistemas de información de la UE, los datos de Europol o las bases de datos de Interpol. Dichas respuestas contendrán únicamente los datos a que tenga acceso el usuario de conformidad con el Derecho de la Unión y nacional.

7. La Comisión adoptará un acto de ejecución para especificar el procedimiento técnico para que el PEB consulte los sistemas informativos de la UE, los datos de Europol y las bases de datos de Interpol, así como el formato de las respuestas del PEB. Dicho acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 70, apartado 2.

Artículo 10

Conservación de registros

1. Sin perjuicio de los artículos 12 y 18 del Reglamento (UE) 2016/1862, el artículo 29 del Reglamento (UE) 2019/816 y el artículo 40 del Reglamento (UE) 2016/794, eu-LISA conservará los registros de todas las operaciones de tratamiento de datos en el RCDI. Dichos registros incluirán lo siguiente:

a) el Estado miembro o la agencia de la Unión que inicia la consulta y el perfil de usuario del PEB utilizado, conforme al artículo 8;

b) la fecha y hora de la consulta;

c) los sistemas de información de la UE y los datos de Europol consultados.

2. Cada Estado miembro llevará un registro de las consultas que hacen sus autoridades y el personal de dichas autoridades debidamente autorizado para utilizar el PEB. Cada agencia de la Unión llevará un registro de las consultas que efectúe su personal debidamente autorizado.

3. Los registros a que se refieren los apartados 1 y 2 únicamente se podrán utilizar para la supervisión de la protección de datos, lo que incluye la comprobación del cumplimiento de los requisitos de la consulta y de la legalidad del tratamiento de datos, y para la garantía de la seguridad y la integridad de los datos. Dichos registros estarán protegidos por medidas adecuadas contra el acceso no autorizado y serán suprimidos un año después de su creación. No obstante, en caso de que sean necesarios para procedimientos de supervisión que ya hayan dado comienzo, se suprimirán cuando dejen de ser necesarios para dichos procedimientos de supervisión.

Artículo 11

Procedimientos alternativos en caso de imposibilidad técnica de utilizar el portal europeo de búsqueda

1. Cuando por un fallo del PEB resulte técnicamente imposible utilizar el PEB para consultar uno o varios de los sistemas de información de la UE, o el RCDI, eu-LISA lo notificará a los usuarios del PEB de forma automatizada.

2. Cuando por un fallo de la infraestructura nacional de un Estado miembro resulte técnicamente imposible utilizar el PEB para consultar uno o varios de los sistemas de información de la UE o el RCDI, ese Estado miembro lo notificará a eu-LISA y a la Comisión de forma automatizada.

3. En los casos recogidos en los apartados 1 y 2 del presente artículo y hasta que el fallo técnico quede resuelto, no será de aplicación la obligación a que se refiere el artículo 7, apartados 2 y 4, y los Estados miembros accederán a los sistemas de información de la UE, o al RCDI cuando así deban de hacerlo con arreglo al Derecho de la Unión o nacional.

4. Cuando debido a un fallo de la infraestructura de una agencia de la Unión resulte técnicamente imposible utilizar el PEB para consultar uno o varios de los sistemas de información de la UE o el RCDI, dicha agencia lo notificará a eu-LISA y a la Comisión de forma automatizada.

CAPÍTULO III

Servicio de correspondencia biométrica compartido

Artículo 12

Servicio de correspondencia biométrica compartido

1. Se crea un servicio de correspondencia biométrica compartido (SCB compartido), que almacenará plantillas biométricas obtenidas a partir de los datos a que se refiere el artículo 13, almacenados en el RCDI y el SIS, y permitirá consultar datos biométricos a través de varios sistemas de información de la UE, a efectos de apoyar al RCDI y al DIM y los objetivos del SES, el VIS, Eurodac, el SIS y el ECRIS-TCN.

2. El SCB compartido se compondrá de:

a) una infraestructura central que sustituirá a los sistemas centrales del SES, el VIS, el SEIAV, Eurodac y el ECRIS-TCN, respectivamente, en la medida en que deberá almacenar plantillas biométricas y permitir la búsqueda con datos biométricos;

b) una infraestructura de comunicación segura entre el SCB compartido, el SIS Central y el RCDI.

3. eu-LISA desarrollará el SCB compartido y garantizará su gestión técnica.

Artículo 13

Almacenamiento de plantillas biométricas en el servicio de correspondencia biométrica compartido

1. El SCB compartido almacenará las plantillas biométricas que obtendrá de los siguientes datos biométricos:

a) los datos a que se refiere el artículo 20, apartado 3, letras w) e y), excluidos los datos de impresiones palmares del Reglamento (UE) 2018/1862;

b) los datos a que se refieren el artículo 5, apartados 1, letra b), y 2 del Reglamento (UE) 2019/816.

Las plantillas biométricas se almacenarán en el SCB compartido separadas de un modo lógico, según el sistema de información de la UE del que provengan los datos.

2. Para cada conjunto de datos a que se refiere el apartado 1, el SCB compartido incluirá en cada plantilla biométrica una referencia a los sistemas de información de la UE en que están almacenados los datos biométricos correspondientes y una referencia a los registros reales de dichos sistemas de información de la UE.

3. Las plantillas biométricas solo podrán introducirse en el SCB compartido tras un control de calidad automatizado de los datos biométricos añadidos a uno de los sistemas de información de la UE con que cuenta el SCB compartido para cerciorarse de que se alcanza un estándar mínimo de calidad de los datos.

4. El almacenamiento de los datos mencionados en el apartado 1 cumplirá los estándares de calidad a que se refiere el artículo 37, apartado 2.

5. La Comisión establecerá mediante un acto de ejecución los requisitos de rendimiento y las disposiciones prácticas para supervisar el funcionamiento del SCB compartido, a fin de garantizar que la eficacia de las búsquedas biométricas respete procedimientos en los que el tiempo es un factor crítico, como los controles y las identificaciones en las fronteras. Dicho acto de ejecución se adoptará de conformidad con el procedimiento de examen a que se refiere el artículo 70, apartado 2.

Artículo 14

Búsqueda de datos biométricos con el servicio de correspondencia biométrica compartido

A fin de buscar los datos biométricos almacenados en el RCDI y el SIS, estos utilizarán las plantillas biométricas almacenadas en el SCB compartido. Las consultas con datos biométricos tendrán lugar de conformidad con los fines previstos en el presente Reglamento y en los Reglamentos (CE) n.º 767/2008, (UE) 2017/2226, (UE) 2018/1860, (UE) 2018/1861, (UE) 2018/1862 y (UE) 2019/816.

Artículo 15

Conservación de datos en el servicio de correspondencia biométrica compartido

Los datos a que se refiere el artículo 13, apartados 1 y 2 solo estarán almacenados en el SCB compartido mientras los datos biométricos correspondientes estén almacenados en el RCDI o en el SIS. Los datos se suprimirán del SCB compartido de forma automatizada.

Artículo 16

Conservación de registros

1. Sin perjuicio de los artículos 12 y 18 del Reglamento (UE) 2018/1862 y el artículo 29 del Reglamento (UE) 2019/816, eu-LISA conservará los registros de todas las operaciones de tratamiento de datos dentro del el SCB compartido. Dichos registros incluirán lo siguiente:

a) el Estado miembro o la agencia de la Unión que inicie la consulta;

b) el historial de creación y almacenamiento de las plantillas biométricas;

c) una referencia a los sistemas de información de la UE consultados con las plantillas biométricas almacenadas en el SCB compartido;

d) la fecha y hora de la consulta;

e) el tipo de datos biométricos utilizados para iniciar la consulta;

f) los resultados de la consulta y la fecha y hora de los resultados.

2. Cada Estado miembro y agencia de la Unión llevará un registro de las consultas de la autoridad y del personal debidamente autorizado para utilizar el PEB compartido. Cada agencia de la Unión llevará un registro de las consultas que efectúe su personal debidamente autorizado.

3. Los registros a que se refieren los apartados 1 y 1 *bis* únicamente podrán utilizarse para la supervisión de la protección de datos, lo que incluye la comprobación del cumplimiento de los requisitos de la consulta y de la legalidad del tratamiento de datos, y para la garantía de la seguridad y la integridad de los datos. Dichos registros estarán protegidos por medidas adecuadas contra el acceso no autorizado y serán suprimidos un año después de su creación. No obstante, en caso de que sean necesarios para procedimientos de supervisión que ya hayan dado comienzo, se suprimirán cuando dejen de ser necesarios para dichos, salvo que sean necesarios para procedimientos de supervisión que ya hayan dado comienzo, en cuyo caso se suprimirán una vez que los procedimientos de supervisión ya no exijan dichos registros.

CAPÍTULO IV

Registro común de datos de identidad

Artículo 17

Registro común de datos de identidad

1. Se crea un registro común de datos de identidad (RCDI), que creará un expediente individual para cada persona registrada en el SES, el VIS, el SEIAV, Eurodac o el ECRIS-TCN y contendrá los datos a que se refiere el artículo 18, con el fin de facilitar la identificación correcta de las personas registradas en el SES, el VIS, el SEIAV] Eurodac y el ECRIS-TCN y ayudar a ella, de conformidad con el artículo 20, de apoyar el funcionamiento del DIM, de conformidad con el artículo 21, y de facilitar y racionalizar el acceso por parte de las autoridades designadas y de Europol al SES, al VIS, al SEIAV y a Eurodac, cuando sea necesario con fines de prevención, detección o investigación de delitos terroristas u otros delitos graves de conformidad con el artículo 22.

2. El RCDI se compondrá de:

a) una infraestructura central que sustituirá a los sistemas centrales del SES, el VIS, el SEIAV, Eurodac y el ECRIS-TCN, respectivamente, en la medida en que deberá almacenar los datos a que se refiere el artículo 18;

b) un canal de comunicación seguro entre el RCDI, los Estados miembros y las agencias de la Unión que tengan derecho a utilizar el RCDI de conformidad con el Derecho de la Unión y nacional;

c) una infraestructura de comunicación segura entre el RCDI y el SES, el VIS, el SEIAV, Eurodac y el ECRIS-TCN, así como las infraestructuras centrales del PEB, el SCB compartido y el DIM.

3. eu-LISA desarrollará el RCDI y garantizará su gestión técnica.

4. Cuando, a causa de un fallo del RCDI resulte técnicamente imposible consultar el RCDI para identificar a una persona de conformidad con el artículo 20, detectar identidades múltiples de conformidad con el artículo 21, o a efectos de prevención, detección o investigación de delitos de terrorismo u otros delitos graves de conformidad con el artículo 22, eu-LISA informará a los usuarios del RCDI de manera automatizada.

5. eu-LISA, en colaboración con los Estados miembros, desarrollará un documento de control de interfaces sobre la base del UMF a que se refiere el artículo 38 para el RCDI.

Artículo 18

Datos del registro común de datos de identidad

1. El RCDI almacenará, separados de un modo lógico, los siguientes datos, según el sistema de información del que provengan: los datos a que se refiere el artículo 5, apartados 1, letra b), y 2, y los siguientes datos enumerados en el artículo 5, apartado 1, letra a) del Reglamento (UE) 2019/816: apellido(s); nombre(s) (de pila), fecha de nacimiento; lugar de nacimiento (localidad y país); nacionalidad o nacionalidades; género y, cuando proceda, nombre(s) anterior(es), seudónimo(s) y/o alias, e información sobre los documentos de viaje, si está disponible.

2. Para cada conjunto de datos contemplado en el apartado 1, el RCDI incluirá una referencia a los sistemas de información de la UE a los que pertenecen los datos.

3. Las autoridades que accedan al RCDI deberán hacerlo de conformidad con sus derechos de acceso, tal como se contempla en los instrumentos jurídicos que rigen los sistemas de información de la UE y en el Derecho nacional y de conformidad con sus derechos de acceso con arreglo al presente Reglamento para los fines contemplados en los artículos 20, 21 y 22.

4. Para cada conjunto de datos contemplado en el apartado 1, el RCDI incluirá una referencia al registro efectivo en los sistemas de información de la UE a los que pertenecen los datos.

5. El almacenamiento de los datos mencionados en el apartado 1 cumplirá los estándares de calidad a que se refiere el artículo 37, apartado 2.

Artículo 19

Adición, modificación y eliminación de datos en el registro común de datos de identidad

1. Cuando se añadan, modifiquen o eliminen datos en Eurodac o en el ECRIS-TCN, los datos contemplados en el artículo 18 almacenados en el expediente individual del RCDI se añadirán, modificarán o eliminarán en consecuencia, de forma automatizada.

2. Cuando se cree un vínculo blanco o rojo en el DIM, de conformidad con los artículos 32 o 33, entre los datos de dos o más de los sistemas de información de la UE que constituyen el RCDI, el RCDI añadirá los nuevos datos al expediente individual de los datos vinculados, en lugar de crear un nuevo expediente individual.

Artículo 20

Acceso al registro común de datos de identidad a efectos de identificación

1. La consulta del RCDI será efectuada por una autoridad policial de conformidad con los apartados 2 y 5 exclusivamente en una de las circunstancias siguientes:

a) cuando una autoridad policial no sea capaz de identificar a una persona debido a la falta de un documento de viaje o de otro documento fiable que demuestre su identidad;

b) cuando existan dudas sobre los datos de identidad facilitados por dicha persona;

c) cuando existan dudas en cuanto a la autenticidad del documento de viaje u otro documento fiable facilitado por dicha persona;

d) cuando existan dudas en cuanto a la identidad del titular del documento de viaje u otro documento fiable, o

e) cuando la persona no pueda o se niegue a cooperar.

Dicha consulta no estará permitida en el caso de menores de doce años, de no ser en el interés superior del menor.

2. Cuando se dé alguna de las circunstancias previstas y las medidas legislativas nacionales a que se refiere el apartado 2 las faculten para ello, las autoridades policiales podrán, únicamente con fines de identificación de una persona, consultar el RCDI con los datos biométricos de dicha persona tomados en vivo durante un control de identidad, siempre que el procedimiento se haya iniciado en presencia de esta.

3. Cuando la búsqueda ponga de manifiesto que los datos de esa persona están almacenados en el RCDI, las autoridades policiales tendrán acceso para consultar los datos a que se refiere el artículo 18, apartado 1.

Cuando no puedan utilizarse los datos biométricos de la persona o cuando la consulta de esos datos sea infructuosa, la consulta se llevará a cabo con los datos de identidad de dicha persona en combinación con los datos del documento de viaje, o con los datos de identidad facilitados por esa persona.

4. Cuando las autoridades policiales de un Estado miembro hayan sido habilitadas para ello por medidas legislativas nacionales conforme al apartado 6, podrán consultar el RCDI con los datos biométricos de dichas personas, en caso de catástrofe natural, accidente o ataque terrorista y únicamente con el fin de identificar a personas desconocidas que no puedan identificarse o restos humanos no identificados.

5. Los Estados miembros que deseen acogerse a la posibilidad prevista en el apartado 1 adoptarán medidas legislativas nacionales al efecto. Al hacerlo, los Estados miembros tendrán en cuenta la necesidad de evitar cualquier discriminación de los nacionales de terceros países. Esas medidas legislativas especificarán los objetivos precisos de la identificación dentro de los fines mencionados en el artículo 2, apartado 1, letras b) y c). Designarán a las autoridades policiales competentes y establecerán los procedimientos, condiciones y criterios de dichos controles.

6. Los Estados miembros que deseen hacer uso de la posibilidad prevista en el apartado 1 *ter* adoptarán medidas legislativas nacionales que establezcan los procedimientos, las condiciones y los criterios.

Artículo 21

Acceso al registro común de datos de identidad para la detección de identidades múltiples

1. Cuando una consulta del RCDI resulte en un vínculo amarillo de conformidad con el artículo 28, apartado 4, la autoridad responsable de la verificación manual de manual de identidades diferentes, determinada de conformidad con el artículo 29, podrá acceder, únicamente a efectos de dicha verificación, a los datos a que se refiere el artículo 18, apartados 1 y 2 almacenados en el RCDI pertenecientes a los distintos sistemas de información de la UE conectados a un vínculo amarillo.

2. Cuando una consulta del RCDI resulte en un vínculo rojo de conformidad con el artículo 32, las autoridades a que se refiere el artículo 26, apartado 2, podrán acceder, únicamente a efectos de combatir la usurpación de identidad, a los datos a que se refiere el artículo 18, apartado 1 y 2, almacenados en el RCDI pertenecientes a los distintos sistemas de información de la UE conectados por un vínculo rojo.

Artículo 22

Consulta del registro común de datos de identidad con fines de prevención, detección o investigación de delitos de terrorismo u otros delitos graves

1. En un caso específico, las autoridades designadas y Europol podrán consultar el RCDI cuando existan motivos razonables para creer que la consulta de los sistemas de información de la UE contribuirá a la prevención, detección o investigación de los delitos de terrorismo u otros delitos graves, en particular cuando exista una sospecha fundada de que el sospechoso, autor o víctima de un delito de terrorismo u otro delito grave es una persona cuyos datos se almacenan en Eurodac, para obtener información sobre si en Eurodac se encuentran datos sobre una persona específica.

2. Cuando, en respuesta a una consulta, el RCDI indique que existen datos sobre esa persona en Eurodac, el RCDI proporcionará a las autoridades designadas y a Europol una respuesta en forma de una referencia, de las mencionadas en el artículo 18, apartado 2, que indique que Eurodac contiene los datos objeto de correspondencia. El RCDI responderá de manera que la seguridad de los datos no se vea comprometida.

La respuesta en la que se indique que los datos sobre esa persona se encuentran en Eurodac se utilizará únicamente a efectos de la presentación de una solicitud de pleno acceso con arreglo a las condiciones y procedimientos establecidos en los instrumentos jurídicos respectivos que rigen dicho acceso.

En caso de una correspondencia o de múltiples correspondencias, la autoridad designada o Europol presentará una solicitud de pleno acceso al menos a uno de los sistemas de información con los que se haya generado una correspondencia.

Cuando, con carácter excepcional, no se solicite el pleno acceso, las autoridades designadas deberán consignar la justificación para no hacerlo, en el fichero nacional, y Europol registrará la justificación en el expediente correspondiente.

3. El pleno acceso a los datos contenidos en Eurodac para los fines de prevención, detección o investigación de los delitos de terrorismo u otros delitos graves seguirá estando sujeto a las condiciones y los procedimientos establecidos en los respectivos instrumentos jurídicos que regulen dicho acceso.

Artículo 23

Conservación de los datos en el registro común de datos de identidad

1. Los datos a que se refiere el artículo 18, apartados 1, 2 y 4, se eliminarán del registro común de datos de identidad (RCDI) de forma automatizada de conformidad con las disposiciones de conservación de los datos del Reglamento (UE) 2019/816.

2. El expediente individual se almacenará en el RCDI sólo durante el mismo tiempo que los datos correspondientes permanezcan almacenados en al menos uno de los sistemas de información de la UE cuyos datos estén contenidos en el RCDI. La creación de un vínculo no afectará al periodo de conservación de cada uno de los datos vinculados.

Artículo 24

Conservación de registros

1. Sin perjuicio del artículo 29 del Reglamento (UE) 2019/816, eu-LISA conservará los registros de todas las operaciones de tratamiento de datos dentro del RCDI de conformidad con los apartados 2, 3 y 4 del presente artículo.

2. eu-LISA conservará los registros de todas las operaciones de tratamiento de datos en el RCDI con arreglo al artículo 20. Dichos registros incluirán lo siguiente:

-a) el Estado miembro o la agencia de la Unión que inicie la consulta;

b) la finalidad del acceso del usuario que realice la consulta a través del RCDI;

c) la fecha y hora de la consulta;

d) el tipo de datos utilizados para iniciar la consulta;

e) los resultados de la consulta.

3. eu-LISA conservará los registros de todas las operaciones de tratamiento de datos en el RCDI con arreglo al artículo 21. Dichos registros incluirán lo siguiente:

a) el Estado miembro o la agencia de la Unión que inicie la consulta;

b) la finalidad del acceso del usuario que realice la consulta a través del RCDI;

c) la fecha y hora de la consulta;

d) cuando se genere un vínculo, el tipo de datos utilizados para iniciar la consulta y los resultados de la consulta indicando el sistema de información de la UE del que se recibieron los datos.

4. eu-LISA conservará los registros de todas las operaciones de tratamiento de datos en el RCDI con arreglo al artículo 22. Dichos registros incluirán lo siguiente:

a) la fecha y hora de la consulta;

b) los datos utilizados para iniciar la consulta;

c) los resultados de la consulta;

d) el Estado miembro o la agencia de la Unión que consulte el RCDI.

La autoridad de control competente de conformidad con el artículo 41 de la Directiva (UE)2016/680, o el Supervisor Europeo de Protección de Datos de conformidad con el artículo 43 del Reglamento (UE) 2016/794, verificará periódicamente los registros de dichos accesos, a intervalos no superiores a seis meses, con el fin de cerciorarse del cumplimiento de los procedimientos y condiciones establecidos en el artículo 22, apartados 1 y 2 del presente Reglamento.

5. Cada Estado miembro conservará los registros de las consultas que efectúen sus autoridades y el personal de esas autoridades debidamente autorizadas para utilizar el RCDI en virtud de los artículos 20, 21 y 22. Cada agencia de la Unión llevará registros de las consultas que efectúe su personal debidamente autorizado en virtud de los artículos 21 y 22.

Además, para cualquier acceso al RCDI con arreglo al artículo 22, cada Estado miembro conservará los registros siguientes:

a) el número de referencia del expediente nacional;

b) el motivo del acceso;

c) de conformidad con las normas nacionales, el nombre único de usuario del funcionario que haya efectuado la búsqueda y el del funcionario que haya pedido la búsqueda.

6. Con arreglo al Reglamento (UE) 2016/794, para cualquier acceso al RCDI con arreglo al artículo 22 del presente Reglamento, Europol conservará registros de la identidad del usuario único del funcionario que haya realizado la consulta y del funcionario que haya encargado la consulta.

7. Los registros contemplados en los apartados 2 a 6 únicamente podrán utilizarse para la supervisión de la protección de datos, lo que incluye la comprobación del cumplimiento de las condiciones de la consulta y de la legalidad del tratamiento de datos, y para la garantía de la seguridad y la integridad de los datos. Esos registros estarán protegidos por medidas adecuadas contra el acceso no autorizado y serán suprimidos un año después de su creación, salvo que sean necesarios para procedimientos de supervisión que ya hayan dado comienzo, en cuyo caso se suprimirán cuando dejen de ser necesarios para dichos procedimientos de supervisión.

8. eu-LISA conservará los registros relativos al historial de los datos en expedientes individuales. eu-LISA suprimirá esos registros de manera automatizada, una vez que se hayan suprimido esos datos.

CAPÍTULO V

Detector de identidades múltiples

Artículo 25

Detector de identidades múltiples

1. A fin de apoyar el funcionamiento del RCDI y la consecución de los objetivos del SES, el VIS, el SEIAV, Eurodac, el SIS y el ECRIS-TCN, se establece un detector de identidades múltiples (DIM), para crear y almacenar los expedientes de confirmación de identidad a que se refiere el artículo 34, que contenga vínculos entre los datos de los sistemas de información de la UE incluidos en el RCDI y el SIS y, permita la detección de identidades múltiples con el doble objetivo de facilitar los controles de identidad y combatir la usurpación de identidad.

2. El DIM se compondrá de:

a) una infraestructura central, que almacenará los vínculos y las referencias a los sistemas de información de la UE;

b) una infraestructura de comunicación segura que conecte el DIM con el SIS y las infraestructuras centrales del PEB y el RCDI.

3. eu-LISA desarrollará el DIM y garantizará su gestión técnica.

Artículo 26

Acceso al detector de identidades múltiples

1. A los efectos de la verificación manual de diferentes identidades a que se refiere el artículo 29, se concederá el acceso a los datos contemplados en el artículo 34 almacenados en el DIM a:

a) las oficinas Sirene del Estado miembro que cree o actualice una descripción con arreglo al Reglamento (UE) 2018/1862;

b) las autoridades centrales del Estado miembro que ha dictado la condena, al anotar o modificar datos en el ECRIS-TCN de conformidad con los artículos 5 o 9 del Reglamento E(UE) 2019/816.

2. Las autoridades de los Estados miembros y las agencias de la Unión que tengan acceso a, como mínimo, un sistema de información de la UE incluido en el RDCI o al SIS tendrán acceso a los datos a que se refiere el artículo 34, letras a) y b), en lo relativo a los vínculos rojos según el artículo 32.

3. Las autoridades de los Estados miembros y las agencias de la Unión tendrán acceso a los vínculos blancos mencionados en el artículo 33 cuando tengan acceso a los dos sistemas de información de la UE que contengan los datos entre los que se haya establecido el vínculo blanco.

4. Las autoridades de los Estados miembros y las agencias de la Unión tendrán acceso a los vínculos verdes a que se refiere el artículo 31 cuando tengan acceso a los dos sistemas de información de la UE que contengan los datos entre los que se haya establecido el vínculo verde y una consulta de dichos sistemas de información haya revelado una correspondencia con los dos conjuntos de datos relacionados.

Artículo 27

Detector de identidades múltiples

1. Se iniciará una detección de identidades múltiples en el RCDI y el SIS cuando:

a) se cree o actualice una descripción sobre una persona en el SIS de conformidad con los capítulos VI a IX del Reglamento (UE) 2018/1862;

b) se cree o modifique un registro de datos en el ECRIS-TCN de conformidad con los artículos 5 o 9 del Reglamento (UE) 2019/ 816.

2. Cuando los datos contenidos en un sistema de información de la UE mencionado en el apartado 1 contengan datos biométricos, el RCDI y el SIS Central utilizarán el SCB compartido para realizar la detección de identidades múltiples. El SCB compartido comparará las plantillas biométricas obtenidas a partir de cualquier nuevo dato biométrico con las plantillas biométricas ya contenidas en el SCB compartido, con el fin de verificar si los datos pertenecientes a una misma persona están ya almacenados en el RCDI o en el SIS Central.

3. Además del proceso mencionado en el apartado 2, el RDCI y el SIS Central utilizarán el PEB para buscar los datos almacenados en el SIS Central y el RDCI, respectivamente, utilizando los datos siguientes:

a) apellido(s); nombre (s); apellido(s) de soltero, nombres usados con anterioridad y alias; fecha de nacimiento, lugar de nacimiento, género y cualquier nacionalidad(es) tal como se definen en el artículo 20, apartado 3, letra a), del Reglamento (UE) 2018/1862;

b) apellido(s); nombre(s) (de pila), fecha de nacimiento, lugar de nacimiento (localidad y país), nacionalidad(es) y género tal como se definen en el artículo 5, apartado 1, letra a), del Reglamento (UE) 2019/816.

4. Además del proceso mencionado en los apartados 2 y 3, el RDCI y el SIS Central utilizarán el PEB para buscar los datos almacenados en el RDCI y en el SIS Central, respectivamente, utilizando los datos del documento de viaje.

5. La detección de identidades múltiples únicamente se iniciará con el fin de comparar los datos disponibles en un sistema de información de la UE con los datos disponibles en otros sistemas de información de la UE.

Artículo 28

Resultados de la detección de identidades múltiples

1. Si las consultas a que se refiere el artículo 27, apartados 2, 3 y 4, no dan lugar a ninguna correspondencia, los procedimientos a que se refiere el artículo 27, apartado 1, continuarán de conformidad con los instrumentos jurídicos por los que se rigen.

2. Cuando la consulta establecida en el artículo 27, apartados 2, 3 y 4, dé lugar a una o más correspondencias, el RCDI y, cuando proceda, el SIS crearán un vínculo entre los datos utilizados para iniciar la consulta y los datos que hayan dado lugar a la correspondencia.

Cuando se registren varias correspondencias, se creará un vínculo entre todos los datos que hayan dado lugar a una correspondencia. Cuando los datos ya se hubiesen vinculado establece previamente, el vínculo existente se extenderá a los datos utilizados para iniciar la consulta.

3. Cuando la consulta a que se refiere el artículo 27, apartados 2, 3 y 4, dé lugar a una o varias correspondencias y los datos de identidad de los expedientes vinculados sean los mismos o similares, se creará un vínculo blanco de conformidad con el artículo 33.

4. Cuando la consulta a que se refiere el artículo 27, apartados 2, 3 y 4, dé lugar a una o varias correspondencias y los datos de identidad de los expedientes vinculados no puedan considerarse similares, se creará un vínculo amarillo de conformidad con el artículo 30 y será de aplicación el procedimiento a que se refiere el artículo 29.

5. La Comisión adoptará actos delegados de conformidad con el artículo 69 por los que se establezcan los procedimientos para determinar los casos en que pueda considerarse que los datos de identidad son los mismos o similares.

6. Los vínculos se almacenarán en el expediente de confirmación de identidad a que se refiere el artículo 34.

7. La Comisión, en cooperación con eu-LISA, establecerá mediante actos de ejecución las normas técnicas para crear vínculos entre los datos de los distintos sistemas de información de la UE. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 70, apartado 2.

Artículo 29

Verificación manual de identidades diferentes y autoridades responsables

1. Sin perjuicio del apartado 2, la autoridad responsable de la verificación manual de verificación de identidades diferentes será:

a) la oficina Sirene del Estado miembro, en caso de correspondencias que se produzcan al crear o actualizar una descripción en el SIS con arreglo al Reglamento (UE) 2018/1862;

b) las autoridades centrales del Estado miembro que ha dictado la condena, en caso de correspondencias que se produzcan al registrar o modificar datos en el ECRIS-TCN de conformidad con los artículos 5 o 9 del Reglamento (UE) 2019/816.

El DIM indicará la autoridad responsable de la verificación manual de las identidades diferentes que figuren en el expediente de confirmación de identidad.

2. La autoridad responsable de la verificación manual de las diferentes identidades en el expediente de confirmación de identidad será la oficina Sirene del Estado miembro que haya creado la descripción, cuando se cree un vínculo a los datos contenidos en una descripción:

a) respecto de personas buscadas para su detención o a efectos de su entrega o extradición, según el artículo 26 del Reglamento (UE) 2018/1862;

b) respecto de personas desaparecidas o vulnerables, según el artículo 32 del Reglamento (UE) 2018/1862;

c) respecto de personas buscadas para su participación en un proceso judicial, según el artículo 34 del Reglamento (UE) 2018/1862;

d) respecto de personas para controles discretos, controles de investigación o controles específicos, según el artículo 36 del Reglamento (UE) 2018/1862.

3. La autoridad responsable de la verificación manual de las diferentes identidades tendrá acceso a los datos vinculados contenidos en el expediente de confirmación de identidad pertinente y a los datos de identidad vinculados en los sistemas de información pertinentes, así como, cuando proceda, en el SIS. Evaluará las diferentes identidades sin demora. Una vez finalizada dicha evaluación, actualizará el vínculo en consonancia con los artículos 31, 32 y 33 y lo añadirá sin demora al expediente de confirmación de identidad.

4. Cuando se cree más de un vínculo, la autoridad responsable de la verificación manual de las diferentes identidades evaluará cada uno por separado.

5. Cuando los datos que den lugar a una correspondencia estén previamente vinculados, la autoridad responsable de la verificación manual de las diferentes identidades tendrá en cuenta los vínculos existentes al evaluar la creación de nuevos vínculos.

Artículo 30

Vínculo amarillo

1. Cuando no haya tenido lugar una verificación manual de identidades diferentes, un vínculo entre datos procedentes de dos o más sistemas de información de la UE se clasificará como amarillo en cualquiera de los siguientes casos:

a) cuando los datos vinculados compartan los mismos datos biométricos, pero tengan datos de identidad similares o distintos;

b) cuando los datos vinculados contengan distintos datos de identidad, pero compartan los mismos datos del documento de viaje y al menos uno de los sistemas de información de la UE no contenga datos biométricos de la persona de que se trate;

c) cuando los datos vinculados contengan los mismos datos de identidad, pero tengan distintos datos biométricos;

d) cuando los datos vinculados contengan datos de identidad similares o distintos, los mismos datos del documento de viaje, pero tengan distintos datos biométricos.

2. Cuando un vínculo se clasifique como amarillo con arreglo a el apartado 1, será de aplicación el procedimiento previsto en el artículo 29.

Artículo 31

Vínculo verde

1. Un vínculo entre datos procedentes de dos o más sistemas de información de la UE se clasificará como verde cuando:

a) los datos vinculados contengan datos biométricos diferentes, pero compartan los mismos datos de identidad y la autoridad responsable de la verificación manual de las identidades diferentes haya concluido que los datos vinculados hacen referencia a dos personas distintas;

b) los datos vinculados contengan diferentes datos biométricos, contengan datos de identidad similares o distintos, compartan los mismos datos del documento de viaje y la autoridad responsable de la verificación manual de las identidades diferentes haya concluido que los datos vinculados hacen referencia a dos personas distintas;

c) los datos vinculados contengan distintos datos de identidad, pero compartan los mismos datos del documento de viaje, al menos uno de los sistemas de información de la UE no contenga datos biométricos de la persona de que se trate y la autoridad responsable de la verificación manual de las identidades diferentes haya concluido que los datos vinculados hacen referencia a dos personas distintas.

2. Cuando se consulten el RCDI o el SIS y exista un vínculo verde entre dos o más de los sistemas de información de la UE que constituyen el RCDI o con el SIS, el DIM indicará que los datos de identidad de los datos vinculados no corresponden a la misma persona.

3. Si una autoridad de un Estado miembro tiene pruebas que sugieran que un vínculo verde ha sido registrado incorrectamente en el DIM, no está actualizado o el tratamiento de datos en el DIM o en los sistemas de información de la UE es contrario al presente Reglamento, comprobará los datos pertinentes almacenados en el RCDI y el SIS y, en caso necesario, rectificará o suprimirá sin demora el vínculo en el DIM. Dicha autoridad del Estado miembro informará sin demora al Estado miembro responsable de la verificación manual de las identidades diferentes.

Artículo 32

Vínculo rojo

1. Un vínculo entre datos procedentes de dos o más sistemas de información de la UE se clasificará como rojo en cualquiera de los siguientes casos:

a) cuando los datos vinculados compartan los mismos datos biométricos, pero contengan datos de identidad similares o distintos, y la autoridad responsable de la verificación manual de las identidades diferentes haya concluido que los datos vinculados hacen referencia a la misma persona de manera injustificada;

b) cuando los datos vinculados contengan los mismos datos de identidad o datos de identidad similares o distintos y los mismos datos del documento de viaje, pero distintos datos biométricos y la autoridad responsable de la verificación manual de las diferentes identidades haya concluido que los datos vinculados hacen referencia a dos personas diferentes, al menos una de las cuales está utilizando el mismo documento de viaje de manera injustificada;

c) cuando los datos vinculados compartan los mismos datos de identidad, pero contengan distintos datos biométricos y la autoridad responsable de la verificación manual de las identidades diferentes haya concluido que los datos vinculados hacen referencia a dos personas distintas de manera injustificada;

d) cuando los datos vinculados contengan distintos datos de identidad, pero compartan los mismos datos del mismo documento de viaje, al menos uno de los sistemas de información de la UE no contenga datos biométricos de la persona de que se trate y la autoridad responsable de la verificación manual de las diferentes identidades haya concluido que los datos vinculados hacen referencia a la misma persona de manera injustificada.

2. Cuando se consulten el registro común de datos de identidad (RCDI) o el SIS y exista un vínculo rojo entre dos o más de los sistemas de información que constituyen el RCDI o con el SIS, el DIM responderá indicando los datos a que se refiere el artículo 34. Las actuaciones subsiguientes a un vínculo rojo se realizarán de conformidad con el Derecho nacional y de la Unión, y cualquier consecuencia jurídica para la persona de que se trate se basará únicamente en los datos pertinentes sobre ella. La mera existencia de un vínculo rojo no tendrá consecuencias jurídicas para la persona afectada.

3. Cuando se cree un vínculo rojo entre datos del SES, el VIS, el SEIAV, Eurodac o el ECRIS-TCN, se actualizará el expediente individual almacenado en el RCDI de conformidad con el artículo 19, apartado 2.

4. Sin perjuicio de las disposiciones relativas al tratamiento de las descripciones en el SIS a que se hace referencia en los Reglamentos (UE) 2018/1860, (UE) 2018/1861 y (UE) 2018/1862, y sin perjuicio de las limitaciones necesarias para proteger la seguridad y el orden público, prevenir la delincuencia y garantizar que ninguna investigación nacional corra peligro, cuando se cree un vínculo rojo, la autoridad encargada de la verificación manual de las diferentes identidades informará a la persona concernida de la existencia ilegal de datos de múltiples identidades y facilitará por escrito a la persona un número de identificación único como se contempla en el artículo 34, letra c), una referencia a la autoridad responsable de la verificación manual de las identidades diferentes como se contempla en el artículo 34, letra d) del presente Reglamento, y la dirección del portal web creado de conformidad con el artículo 49 del presente Reglamento.

5. La autoridad responsable de la verificación manual de las diferentes identidades facilitará por escrito la información a que se refiere el apartado 4 por medio de un formulario normalizado. La Comisión determinará el contenido y la presentación de dicho formulario y las modalidades de la información mediante actos de ejecución. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 70, apartado 2.

6. Cuando se genere un vínculo rojo, el DIM notificará de forma automatizada a las autoridades responsables de los datos vinculados.

7. Cuando una autoridad de un Estado miembro o una agencia de la Unión que tenga acceso al RCDI o al SIS obtenga pruebas que sugieran que un vínculo rojo ha sido registrado incorrectamente en el DIM es incorrecto o que los datos tratados en el DIM, el RCDI o el SIS han sido tratados de manera contraria al presente Reglamento, dicha autoridad comprobará los datos almacenados en el RCDI y en el SIS y, en caso necesario:

a) cuando el vínculo se refiera a una de las descripciones en el SIS a que hace referencia el artículo 29, apartado 2, informará inmediatamente a la oficina Sirene correspondiente del Estado miembro que creó la descripción en el SIS;

b) en todos los demás casos, o rectificará o suprimirá inmediatamente el enlace del DIM.

Si una oficina Sirene es contactada de conformidad con la letra a) del primer párrafo, verificará las pruebas facilitadas por la autoridad del Estado miembro o la Agencia de la Unión y, si procede, rectificará o suprimirá el vínculo en el DIM inmediatamente.

La autoridad del Estado miembro que obtenga las pruebas informará sin demora a la autoridad del Estado miembro responsable de la verificación manual de las identidades diferentes, indicando, en su caso, cualquier rectificación o supresión de un vínculo rojo.

Artículo 33

Vínculo blanco

1. Un vínculo entre datos procedentes de dos o más sistemas de información de la UE se clasificará como blanco en cualquiera de los siguientes casos:

a) cuando los datos vinculados compartan los mismos datos biométricos y datos de identidad iguales o similares;

b) cuando los datos vinculados compartan datos de identidad iguales o similares, los mismos datos del documento de viaje y al menos uno de los sistemas de información de la UE no contenga datos biométricos de la persona;

c) cuando los datos vinculados compartan los mismos datos biométricos y los mismos datos del documento de viaje, pero datos de identidad similares;

d) cuando los datos vinculados compartan los mismos datos biométricos, pero contengan datos de identidad similares o distintos, y la autoridad responsable de la verificación manual de las identidades diferentes haya concluido que los datos vinculados se refieren a la misma persona de manera justificada.

2. Cuando se consulten el RCDI o el SIS y exista un vínculo blanco entre datos de dos o más de los sistemas de información de la UE, el DIM indicará que los datos de identidad de los datos vinculados corresponden a la misma persona. Los sistemas de información de la UE consultados responderán indicando, en su caso, todos los datos vinculados relativos a la persona, dando lugar así a una correspondencia en relación con los datos sujetos al vínculo blanco, cuando la autoridad que inicie la consulta tenga acceso a los datos vinculados con arreglo al Derecho de la Unión o nacional.

3. Cuando se cree un vínculo blanco entre datos del SES, el VIS, el SEIAV, Eurodac o el ECRIS-TCN, se actualizará el expediente individual almacenado en el RCDI de conformidad con el artículo 19, apartado 2.

4. Sin perjuicio de las disposiciones relativas al tratamiento de las descripciones en el SIS a que se hace referencia en los Reglamentos (UE) 2018/1860, (UE) 2018/1861 y (UE) 2018/1862, y sin perjuicio de las limitaciones necesarias para proteger la seguridad y el orden público, prevenir la delincuencia y garantizar que no se ponga en peligro ninguna investigación nacional, cuando se genere un vínculo blanco, a raíz de una verificación manual de identidades diferentes, la autoridad responsable de la verificación manual de las diferentes identidades informará a la persona de que se trate de la existencia de identidades similares y facilitará por escrito a la persona un número de identificación único como se contempla en el artículo 34, letra c) del presente Reglamento, una referencia a la autoridad responsable de la verificación manual de las diferentes identidades como se contempla en el artículo 34, letra d), y la dirección del portal web creado de conformidad con el artículo 49 del presente Reglamento.

5. Si una autoridad de un Estado miembro tiene pruebas que sugieren que un vínculo blanco ha sido registrado incorrectamente, es materialmente inexacto o no está actualizado o que el tratamiento de datos en el DIM o en los sistemas de información de la UE es contrario al presente Reglamento, comprobará los datos pertinentes almacenados en el RCDI y el SIS y, en caso necesario, rectificará o suprimirá sin demora el vínculo en el DIM. Dicha autoridad del Estado miembro informará sin demora al Estado miembro responsable de la verificación manual de las identidades diferentes.

6. La autoridad responsable de la verificación manual de las identidades diferentes facilitará por escrito la información a que se refiere el apartado 4, por medio de un formulario normalizado. La Comisión determinará el contenido y presentación de dicho formulario y las modalidades de la información mediante actos de ejecución. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 70, apartado 2.

Artículo 34

Expediente de confirmación de identidad

El expediente de confirmación de identidad contendrá los datos siguientes:

a) los vínculos, según los artículos 30 a 33;

b) una referencia a los sistemas de información de la UE cuyos datos estén vinculados;

c) un número de identificación único que permita recuperar de los sistemas de información de la UE los datos de los expedientes vinculados correspondientes;

d) la autoridad responsable de la verificación manual de las identidades diferentes;

e) la fecha de creación del vínculo o de cualquier actualización del mismo.

Artículo 35

Conservación de los datos en el detector de identidades múltiples

Los expedientes de confirmación de identidad y los datos en ellos contenidos, incluidos los vínculos, se almacenarán en el DIM únicamente durante el tiempo en que los datos vinculados permanezcan almacenados en dos o más sistemas de información de la UE. Serán suprimidos del DIM de forma automatizada.

Artículo 36

Conservación de registros

1. eu-LISA conservará los registros de todas las operaciones de tratamiento de datos en el DIM. Dichos registros incluirán lo siguiente:

a) el Estado miembro que inicie la consulta;

b) el motivo del acceso del usuario;

c) la fecha y hora de la consulta;

d) el tipo de datos utilizados para iniciar la consulta o consultas;

e) la referencia a los datos vinculados;

f) el historial del expediente de confirmación de identidad.

2. Cada Estado miembro y agencia de la Unión mantendrá un registro de las consultas de la autoridad y del personal debidamente autorizado para utilizar el DIM.

3. Los registros a que se refieren los apartados 1 y 2 únicamente podrán utilizarse para la supervisión de la protección de datos, lo que incluye la comprobación del cumplimiento de los requisitos de la consulta y de la legalidad del tratamiento de datos, y para la garantía de la seguridad y la integridad de los datos. Dichos registros estarán protegidos por medidas adecuadas contra el acceso no autorizado y serán suprimidos un año después de su creación. No obstante, en caso de que sean necesarios para procedimientos de supervisión que ya hayan dado comienzo, se suprimirán una vez que los procedimientos de supervisión ya no exijan ichos registros.

CAPÍTULO VI

Medidas de apoyo a la interoperabilidad

Artículo 37

Calidad de los datos

1. Además de las responsabilidades de los Estados miembros respecto de los datos introducidos en los sistemas, eu-LISA establecerá mecanismos y procedimientos automatizados de control de la calidad de los datos almacenados en el SIS, Eurodac, el ECRIS-TCN, el SCB compartido y el RCDI.

2. eu-LISA aplicará mecanismos para evaluar la exactitud del SCB compartido, indicadores comunes de calidad de los datos y los estándares mínimos de calidad para el almacenamiento de datos en el SIS, Eurodac, el ECRIS-TCN, el SCB compartido y el RCDI.

Solo los datos que respeten las normas mínimas de calidad podrán introducirse en el SIS, Eurodac, el ECRIS-TCN, el SCB compartido, el RCDI y el DIM.

3. eu-LISA presentará a los Estados miembros informes periódicos sobre los mecanismos y procedimientos automatizados de control de la calidad de los datos. eu-LISA también presentará un informe periódico a la Comisión acerca de los problemas detectados y los Estados miembros a los que estos conciernan. eu-Lisa también presentará ese informe al Parlamento Europeo y al Consejo, previa petición. Los informes presentados en virtud del presente apartado no contendrán datos personales.

4. Los pormenores de los mecanismos y procedimientos automatizados de control de la calidad de los datos, los indicadores comunes de la calidad de los datos y los estándares mínimos de calidad para el almacenamiento de datos en el SIS, Eurodac, el ECRIS-TCN, el SCB compartido y el RCDI, en particular en lo relativo a los datos biométricos, se establecerán mediante actos de ejecución. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 70, apartado 2.

5. Un año después de la creación de los mecanismos y procedimientos automatizados de control de la calidad de los datos, los indicadores comunes de calidad de los datos y los estándares mínimos de calidad de los datos, y cada año en lo sucesivo, la Comisión valorará la implementación por los Estados miembros de la calidad de los datos y formulará las recomendaciones necesarias. Los Estados miembros presentarán a la Comisión un plan de acción para subsanar las deficiencias detectadas en el informe de valoración y, en particular, los problemas de calidad de los datos derivados de datos erróneos en los sistemas de información de la UE. Los Estados miembros e informarán periódicamente a la Comisión sobre cualquier progreso relativo a dicho plan de acción hasta que este se aplique plenamente.

La Comisión remitirá el informe de valoración al Parlamento Europeo, al Consejo, al Supervisor Europeo de Protección de Datos, al Comité Europeo de Protección de Datos y a la Agencia de los Derechos Fundamentales de la Unión Europea, establecida por el Reglamento (CE) n.º 168/2007 del Consejo ([37]).

Artículo 38

Formato universal de mensajes

1. Se establece la norma de formato universal de mensajes (UMF). El UMF define una norma para ciertos elementos del contenido del intercambio transfronterizo de información entre sistemas de información, autoridades u organizaciones en el ámbito de la justicia y los asuntos de interior.

([37]) Reglamento (CE) n.º 168/2007 del Consejo, de 15 de febrero de 2007, por el que se crea una Agencia de los Derechos Fundamentales de la Unión Europea (DO L 53 de 22.2.2007, p. 1).

2. La norma UMF se utilizará en el desarrollo de Eurodac, el ECRIS-TCN, el PEB, el RCDI, el DIM y, si procede, en el desarrollo por parte de eu-LISA o de cualquier otra agencia de la Unión de nuevos modelos de intercambio de información y sistemas de información en el ámbito de la justicia y los asuntos de interior.

3. La Comisión adoptará un acto de ejecución para establecer y desarrollar la norma UMF a que se refiere el apartado 1 del presente artículo. Dicho acto de ejecución se adoptará de conformidad con el procedimiento de examen a que se refiere el artículo 70, apartado 2.

Artículo 39

Repositorio central para la presentación de informes y estadísticas

1. Se crea un repositorio central para la presentación de informes y estadísticas (RCIE) con el fin de apoyar los objetivos del SIS y el ECRIS-TCN, de conformidad con los respectivos instrumentos jurídicos que rigen esos sistemas, y de proporcionar datos estadísticos transversales entre sistemas e informes analíticos con fines operativos, de formulación de políticas y de calidad de los datos.

2. eu-LISA establecerá, implementará y alojará en sus sitios técnicos el RCIE que contenga los datos y las estadísticas a que se hace referencia en el artículo 74 del Reglamento (UE) 2018/1862 y el artículo 32 del Reglamento (UE) 2019/816, separados de forma lógica. Los datos contenidos en el RCIE no permitirán la identificación de personas. El acceso al RCIE se concederá por medio de un acceso seguro, con un control de acceso y unos perfiles de usuario específicos, únicamente a efectos de la presentación de informes y estadísticas, a las autoridades a las que se refieren el artículo 74 del Reglamento (UE) 2018/1862 y el artículo 32 del Reglamento (UE) 2019/816.

3. eu-LISA anonimizará los datos y registrará los datos anonimizados en el RCIE. El proceso por el que se anonimizarán los datos será automatizado.

Los datos contenidos en el RCIE no permitirán la identificación de personas.

4. El RCIE se compondrá de:

-a) las herramientas necesarias para anominizar los datos;

a) una infraestructura central, consistente en un repositorio de datos anonimizados;

b) una infraestructura de comunicación segura entre el RCIE y el SIS, Eurodac y el ECRIS-TCN, así como con las infraestructuras centrales del SCB compartido, el RCDI y el DIM.

5. La Comisión adoptará actos delegados de conformidad con el artículo 69 que establezcan normas detalladas sobre el funcionamiento del RCIE, incluidas salvaguardias específicas para el tratamiento de los datos personales a que se refieren los apartados 2 y 3 del presente artículo y las normas de seguridad aplicables al repositorio.

CAPÍTULO VII

Protección de datos

Artículo 40

Responsable del tratamiento

1. En relación con el tratamiento de datos en el SCB compartido, las autoridades de los Estados miembros que sean responsables del tratamiento en Eurodac, el SIS y el ECRIS-TCN, respectivamente, también se considerarán responsables del tratamiento, de conformidad con el artículo 4, apartado 7, del Reglamento (UE) 2016/679, o con el artículo 3, apartado 8, de la Directiva (UE) 2016/680, en lo que respecta a las plantillas biométricas obtenidas a partir de los datos a que se refiere el artículo 13 del presente Reglamento que introduzcan en sus respectivos sistemas y tendrán responsabilidad en el tratamiento de las plantillas biométricas en el SCB compartido.

2. En relación con el tratamiento de datos en el RCDI, las autoridades de los Estados miembros que sean responsables del tratamiento en Eurodac y el ECRIS-TCN, respectivamente, también serán responsables del tratamiento de conformidad con el artículo 4, apartado 7, del Reglamento (UE) 2016/679 o el artículo 3, apartado 8, de la Directiva 2016/680, en lo que respecta a los datos a que se refiere el artículo 18 del presente Reglamento que introduzcan en sus respectivos sistemas y tendrán responsabilidad en el tratamiento de esos datos personales en el RCDI.

3. En relación con el tratamiento de datos en el DIM:

a) la Agencia Europea de la Guardia de Fronteras y Costas será responsable del tratamiento con arreglo al artículo 3, apartado 8, del Reglamento (UE) 2018/1725 en relación con el tratamiento de los datos personales en la unidad central SEIAV;

b) las autoridades de los Estados miembros que añadan o modifiquen datos en el expediente de confirmación de identidad serán responsables del tratamiento de acuerdo con el artículo 4, apartado 7, del Reglamento (UE) 2016/680 o con el artículo 3, apartado 8, de la Directiva (UE) 2016/680, y tendrán responsabilidad en el tratamiento de los datos personales en el DIM.

4. A efectos de la supervisión de la protección de datos, lo que incluye la comprobación del cumplimiento de las condiciones de una consulta y de la legalidad del tratamiento de datos, los controladores de datos tendrán acceso a los registros contemplados en los artículos 10, 16, 24 y 36 para el autocontrol a que se refiere el artículo 45.

Artículo 41

Encargado del tratamiento

En relación con el tratamiento de los datos personales en el SCB compartido, el RCDI y el DIM, eu-LISA será la encargada del tratamiento en el sentido del artículo 3, punto 12, del Reglamento (UE) 2018/1725.

Artículo 42

Seguridad del tratamiento

1. eu-LISA, la unidad central SEIAV, Europol y las autoridades de los Estados miembros garantizarán la seguridad del tratamiento de los datos personales que tenga lugar en virtud de la aplicación del presente Reglamento. eu-LISA, la unidad central SEIAV, Europol y las autoridades de los Estados miembros cooperarán en las tareas relacionadas con la seguridad.

2. Sin perjuicio del artículo 33 del Reglamento (UE) 2018/1725, eu-LISA adoptará las medidas necesarias para garantizar la seguridad de los componentes de interoperabilidad y de su infraestructura de comunicación conexa.

3. En particular, eu-LISA adoptará las medidas necesarias, incluidos un plan de seguridad, un plan de continuidad de las actividades y un plan de recuperación en caso de catástrofe, a fin de:

a) proteger los datos físicamente, entre otras cosas mediante la elaboración de planes de emergencia para la protección de las infraestructuras críticas;

b) denegar a toda persona no autorizada el acceso a los equipos e instalaciones de tratamiento de datos;

c) impedir la lectura, copia, modificación o retirada no autorizadas de los soportes de datos;

d) impedir la introducción no autorizada de datos y la inspección, modificación o eliminación no autorizadas de datos personales registrados;

e) impedir el tratamiento no autorizado de datos y la copia, modificación o eliminación no autorizadas de datos;

f) impedir que los sistemas de tratamiento automatizado de datos sean utilizados por personas no autorizadas por medio de equipos de transmisión de datos;

g) garantizar que las personas autorizadas para acceder a los componentes de interoperabilidad tengan únicamente acceso a los datos cubiertos por su autorización de acceso, exclusivamente mediante identidades de usuario individuales y modos de acceso confidenciales;

h) garantizar la posibilidad de verificar y determinar a qué organismos pueden transmitirse datos personales mediante equipos de transmisión de datos;

i) garantizar la posibilidad de verificar y determinar qué datos han sido tratados en los componentes de interoperabilidad, en qué momento, por quién y con qué fin;

j) impedir la lectura, copia, modificación o eliminación no autorizadas de datos personales durante su transmisión hacia o desde los componentes de interoperabilidad o durante el transporte de soportes de datos, en particular mediante técnicas adecuadas de cifrado;

k) garantizar que, en caso de interrupción, los sistemas instalados puedan volver a funcionar normalmente;

l) garantizar la fiabilidad velando por que se informe adecuadamente de cualquier error de funcionamiento de los componentes de interoperabilidad;

m) controlar la eficacia de las medidas de seguridad mencionadas en el presente apartado y adoptar las medidas de organización del control interno necesarias para garantizar el cumplimiento del presente Reglamento y evaluar dichas medidas de seguridad a la luz de los nuevos avances tecnológicos.

4. Los Estados miembros, Europol y la unidad central SEIAV adoptarán medidas equivalentes a las mencionadas en el apartado 3 en lo que respecta a la seguridad en relación con el tratamiento de datos personales por parte de las autoridades con derecho de acceso a cualquiera de los componentes de interoperabilidad.

Artículo 43

Incidentes de seguridad

1. Cualquier acontecimiento que repercuta o pueda repercutir en la seguridad de los componentes de interoperabilidad y pueda causar daños a los datos almacenados en ellos o la pérdida de dichos datos se considerará un incidente de seguridad, especialmente cuando pueda haber tenido lugar un acceso no autorizado a los datos o cuando la disponibilidad, integridad y confidencialidad de los datos haya sido o pueda haber sido comprometida.

2. Los incidentes de seguridad se gestionarán de forma que se garantice una respuesta rápida, eficaz y adecuada.

3. Sin perjuicio de la notificación y comunicación de una violación de la seguridad de un dato personal de conformidad con el artículo 33 del Reglamento (UE) 2016/679, con el artículo 30 de la Directiva (UE) 2016/680 o con ambos, los Estados miembros notificarán sin demora a la Comisión, a eu-LISA, a las autoridades de control competentes y al Supervisor Europeo de Protección de Datos cualquier incidente de seguridad.

Sin perjuicio de los artículos 34 y 35 del Reglamento (UE) 2018/1725 y en el artículo 34 del Reglamento (UE) 2016/794, el sistema central SEIAV y Europol notificarán sin demora a la Comisión, eu-LISA y el Supervisor Europeo de Protección de Datos cualquier incidente de seguridad.

En el caso de un incidente de seguridad relacionado con la infraestructura central de los componentes de interoperabilidad, eu-LISA lo notificará a la Comisión y al Supervisor Europeo de Protección de Datos.

4. eu-LISA transmitirá sin demora a los Estados miembros, a la unidad central SEIAV y a Europol la información concerniente a un incidente de seguridad que repercuta o pueda repercutir en el funcionamiento de los componentes de interoperabilidad o en la disponibilidad, integridad y confidencialidad de los datos, y presentará un informe en cumplimiento del plan de gestión de incidentes.

5. Los Estados miembros afectados, la unidad central SEIAV, Europol y eu-LISA cooperarán cuando se produzca un incidente de seguridad. La Comisión especificará los detalles de este procedimiento de cooperación mediante actos de ejecución. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 70, apartado 2.

Artículo 44

Autocontrol

Los Estados miembros y las agencias pertinentes de la Unión velarán por que toda autoridad facultada para acceder a los componentes de interoperabilidad adopte las medidas necesarias para controlar su cumplimiento del presente Reglamento y coopere, en caso necesario, con la autoridad de control.

Los responsables del tratamiento de datos a que se refiere el artículo 40 adoptarán las medidas necesarias para controlar la conformidad del tratamiento de datos con el presente Reglamento, incluida la frecuencia de verificación manual de los registros a que se refieren los artículos 10, 16, 24 y 36, y cooperarán, cuando proceda, con las autoridades de control a que se refiere el artículo 49 y con el Supervisor Europeo de Protección de datos a que se refiere el artículo 50.

Artículo 45

Sanciones

Los Estados miembros garantizarán que cualquier uso indebido de datos, tratamiento de datos o intercambio de datos contrario a el presente Reglamento sea sancionable con arreglo al Derecho nacional. Tales sanciones serán efectivas, proporcionadas y disuasorias.

Artículo 46

Responsabilidad

1. Sin perjuicio del derecho a compensación y de la responsabilidad del responsable o el encargado en virtud del Reglamento (EU) 2016/679, la Directiva (UE) 2016/680 y el Reglamento (UE) 2018/1725:

a) cualquier persona o Estado miembro que haya sufrido perjuicios materiales o no materiales como resultado de una operación ilegal de tratamiento de datos personales o cualquier otro acto incompatible con el presente Reglamento por parte de un Estado miembro tendrá derecho a ser indemnizado por dicho Estado miembro;

b) cualquier persona o Estado miembro que haya sufrido perjuicios materiales o no materiales como resultado de un acto de Europol, la Agencia Europea de la Guardia de Fronteras y Costas o eu-LISA incompatible con el presente Reglamento tendrá derecho a recibir una indemnización de la agencia en cuestión.

El Estado miembro en cuestión, Europol, la Agencia Europea de la Guardia de Fronteras y Costas o eu-LISA quedarán exentos, total o parcialmente, de su responsabilidad en virtud del primer párrafo si demuestran que no son responsables del hecho que originó el perjuicio.

2. Si el incumplimiento por un Estado miembro de las obligaciones que le impone el presente Reglamento causa un perjuicio a los componentes de interoperabilidad, dicho Estado miembro será considerado responsable de dicho perjuicio, a no ser que eu-LISA u otro Estado miembro sujeto al presente Reglamento no hayan adoptado las medidas adecuadas para impedir que se produjera el perjuicio o para atenuar sus efectos.

3. Las reclamaciones de indemnización contra un Estado miembro por los perjuicios a los que se refieren los apartados 1 y 2 estarán sujetas al Derecho nacional del Estado miembro demandado. Las reclamaciones de indemnización contra el responsable o contra eu-LISA por los perjuicios a los que se refieren los apartados 1 y 2 estarán sujetas a las condiciones previstas en los Tratados.

Artículo 47

Derecho a la información

1. La autoridad que recoja los datos personales para almacenarlos en el SCB compartido, el RCDI o el DIM, facilitará a las personas cuyos datos se almacenen la información requerida en virtud de los artículos 13 y 14 del Reglamento (UE) 2016/679, los artículos 12 y 13 de la Directiva (UE) 2016/680 y los artículos 15 y 16 del Reglamento (UE) 2018/1725. La autoridad facilitará la información en el momento en el que se recojan dichos datos.

2. Toda la información estará disponible en un lenguaje claro y sencillo y en un idioma que la persona interesada entienda o quepa suponer razonablemente que entiende. Esto incluirá la facilitación de información de un modo apropiado a la edad de los titulares de los datos que sean menores.

3. Las normas sobre el derecho a la información contenidas en las normas aplicables de la Unión en materia de protección de datos se aplicarán a los datos personales registrados en el ECRIS-TCN y tratados a efectos del presente Reglamento.

Artículo 48

Derechos de acceso, rectificación y supresión de datos personales almacenados en el DIM y restricción de su tratamiento

1. Con el fin de ejercer sus derechos en virtud de los artículos 15, 16, 17 y 18 del Reglamento (UE) 2016/679, los artículos 17, 18, 19 y 20 del Reglamento (UE) 2018/1725 y los artículos 14, 15 y 16 de la Directiva (UE) 2016/680, cualquier persona tendrá derecho a dirigirse personalmente a la autoridad competente de cualquier Estado miembro, que deberá examinar la solicitud y darle respuesta.

2. El Estado miembro que hubiere examinado dicha solicitud dará respuesta sin demora injustificada y en cualquier caso en un plazo de cuarenta y cinco días a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros quince días en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El Estado miembro que hubiere examinado dicha solicitud informará al interesado de cualquiera de dichas prórrogas en el plazo de cuarenta y cinco días a partir de la recepción de la solicitud, indicando los motivos de la dilación. Los Estados miembros podrán decidir que las respuestas sean facilitadas por las oficinas centrales.

3. Si se realiza una solicitud de rectificación o supresión de datos personales a un Estado miembro distinto del Estado miembro responsable de la verificación manual de identidades diferentes, el Estado miembro al que se haya realizado la solicitud contactará con las autoridades del Estado miembro responsable de la verificación manual de diferentes identidades en el plazo de siete días. El Estado miembro responsable de la verificación manual de diferentes identidades comprobará la exactitud de los datos y la legalidad de su tratamiento sin demora injustificada y en cualquier caso en el plazo de treinta días desde que se establezca el contacto. Dicho plazo podrá prorrogarse otros quince días en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El Estado miembro responsable de la verificación manual de las identidades diferentes informará al Estado miembro que se haya puesto en contacto con él de cualquier prórroga, así como de las razones que la han motivado. La persona interesada será informada por el Estado miembro que contactó a la autoridad del Estado miembro responsable de la verificación manual de las identidades diferentes acerca del procedimiento ulterior.

4. Si se realiza una solicitud de rectificación o supresión de datos personales a un Estado miembro en el que la unidad central SEIAV fue la responsable de la verificación manual de identidades diferentes, el Estado miembro al que se haya realizado la solicitud contactará por escrito en el plazo de siete días con la unidad central SEIAV y le pedirá que se pronuncie sin demora injustificada y en cualquier caso en el plazo de treinta días desde que se establezca el contacto. Dicho plazo podrá prorrogarse otros quince días en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. La persona interesada será informada por el Estado miembro que contactó a la unidad central SEIAV acerca del procedimiento ulterior.

5. Cuando, previo examen, se compruebe que los datos almacenados en el DIM son inexactos o han sido registrados ilegalmente, el Estado miembro responsable de la verificación manual de las diferentes identidades o, cuando ningún Estado miembro sea responsable de la verificación manual o cuando la unidad central SEIAV sea responsable de la verificación manual de las diferentes identidades, el Estado miembro al que se haya presentado la solicitud corregirá o eliminará esos datos sin demora injustificada. Se informará por escrito al interesado de que sus datos han sido rectificados o suprimidos.

6. Cuando un Estado miembro modifique los datos almacenados en el DIM durante su periodo de validez, dicho Estado miembro llevará a cabo el tratamiento establecido en el artículo 27 y, en su caso, el artículo 29, a fin de determinar si se vincularán los datos modificados. Cuando el tratamiento no dé lugar a ninguna correspondencia, dicho Estado miembro eliminará los datos del expediente de confirmación de identidad. Cuando el tratamiento automatizado dé lugar a una o varias correspondencias, dicho Estado miembro generará o actualizará el vínculo correspondiente de conformidad con las disposiciones pertinentes del presente Reglamento.

7. Cuando el Estado miembro responsable de la verificación manual de diferentes identidades o, cuando proceda, el Estado miembro al que se haya presentado la solicitud no admita que los datos registrados en el DIM son inexactos o han sido ilegalmente registrados, dicho Estado miembro adoptará una decisión administrativa, en la que expondrá por escrito a la persona interesada, sin demora, los motivos para no corregir o eliminar los datos sobre ella.

8. En tal decisión también se informará a la persona interesada de la posibilidad de impugnar la decisión adoptada respecto de la solicitud de acceso, rectificación, restricción de tratamiento o supresión de datos personales, y en su caso se informará sobre cómo interponer una acción judicial o presentar una reclamación ante las autoridades u órganos jurisdiccionales competentes y sobre cualquier tipo de asistencia, en particular de las autoridades nacionales de control.

9. Cualquier solicitud de acceso, rectificación, restricción de tratamiento o supresión de datos personales deberá contener la información necesaria para identificar a la persona en cuestión. Dicha información solo se utilizará para el ejercicio de los derechos recogidos en el presente artículo, tras lo cual se suprimirá inmediatamente.

10. El Estado miembro responsable de la verificación manual de diferentes identidades o, en su caso, el Estado miembro al que se haya realizado la solicitud dejará constancia por escrito de la presentación de una solicitud de acceso, rectificación, restricción de tratamiento o supresión de datos personales y del curso dado a la misma, y pondrá este documento sin demora a disposición de las autoridades nacionales de control.

11. El presente artículo se entiende sin perjuicio de las limitaciones y restricciones a los derechos en él recogidos que establecen el Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680.

Artículo 49

Portal web

1. Se crea un portal web con el fin de facilitar el ejercicio de los derechos de acceso, rectificación, restricción de tratamiento o supresión de datos personales.

2. El portal web contendrá información sobre los derechos y procedimientos a que se refieren los artículos 46 y 47 y una interfaz de usuario que permita a las personas cuyos datos se tratan en el DIM y que han sido informadas de la presencia de un vínculo rojo con arreglo al artículo 32, apartado 4, recibir los datos de contacto de la autoridad competente del Estado miembro responsable de la verificación manual de las identidades diferentes.

3. Para obtener los datos de contacto de la autoridad competente del Estado miembro responsable de la verificación manual de las identidades diferentes, la persona cuyos datos se traten en el DIM debe introducir la referencia a la autoridad responsable de la verificación manual de las identidades diferentes a que se refiere el artículo 34, letra d). El portal web utilizará esta referencia para recuperar los datos de contacto de la autoridad competente del Estado miembro responsable de la verificación manual de las identidades diferentes. El portal web incluirá asimismo un modelo de correo electrónico para facilitar la comunicación entre el usuario del portal y la autoridad competente del Estado miembro responsable de la verificación manual de las identidades diferentes. Dicho correo electrónico incluirá un campo para el número de identificación único a que se refiere el artículo 34, letra c), con el fin de que la autoridad competente del Estado miembro responsable de la verificación manual de las identidades diferentes pueda identificar los datos de que se trate.

4. Los Estados miembros proporcionarán a eu-LISA los datos de contacto de todas las autoridades competentes para examinar y responder a cualquier solicitud contemplada en los artículos 46 y 47 y revisarán periódicamente si estos datos están actualizados.

5. eu-LISA desarrollará el portal web y garantizará su gestión técnica.

6. La Comisión adoptará un acto delegado con arreglo al artículo 69 para adoptar normas detalladas sobre el funcionamiento del portal web, en particular la interfaz de usuario, las lenguas en las que estará disponible el portal y el modelo de correo electrónico.

Artículo 50

Comunicación de datos personales a terceros países, organizaciones internacionales y particulares

Sin perjuicio del artículo 31 del Reglamento (CE) n.º 767/2008, los artículos 25 y 26 del Reglamento (UE) 2016/794, el artículo 41 del Reglamento (UE) 2017/2226 y el artículo 65 del Reglamento (UE) 2018/1240 y de la consulta de bases de datos de Interpol a través del PEB de conformidad con el artículo 9, apartado 5, del presente Reglamento que sean conformes a el capítulo V del Reglamento (UE) 2018/1725 y el capítulo V del Reglamento (UE) 2016/679, los datos personales almacenados en los componentes de interoperabilidad o tratados por ellos o a los que se acceda a través de esos componentes no se transmitirán ni se pondrán a disposición de terceros países, organizaciones internacionales ni entidades privadas.

Artículo 51

Control por parte de las autoridades de control

1. Cada Estado miembro velará por que las autoridades de control supervisen con independencia la legalidad del tratamiento de los datos personales en virtud del presente Reglamento por parte del Estado miembro de que se trate, incluida su transmisión a los componentes de interoperabilidad y desde ellos.

2. Los distintos Estados miembros velarán por que las disposiciones nacionales legislativas, reglamentarias y administrativas adoptadas en virtud de la Directiva (UE) 2016/680 se apliquen también, cuando proceda, al acceso a los componentes de interoperabilidad por parte de las autoridades policiales y de las autoridades designadas, también en relación con los derechos de las personas a cuyos datos se acceda de este modo.

3. Las autoridades de control velarán por que se lleve a cabo una auditoría de las operaciones de tratamiento de datos personales realizadas por las autoridades nacionales responsables para los fines del presente Reglamento, de conformidad con las normas internacionales de auditoría pertinentes, al menos cada cuatro años.

Las autoridades de control publicarán anualmente el número de solicitudes de rectificación o supresión de datos o de limitación del tratamiento de datos personales, las acciones emprendidas posteriormente y el número de rectificaciones, supresiones y limitaciones del tratamiento realizadas en respuesta a solicitudes de las personas afectadas.

4. Los Estados miembros garantizarán que sus autoridades de control dispongan de medios y conocimientos técnicos suficientes para desempeñar las tareas que les encomienda el presente Reglamento.

5. Los Estados miembros proporcionarán la información que les solicite cualquiera de las autoridades de control a que se refiere el artículo 51, apartado 1, del Reglamento (UE) 2016/679 y, en particular, la información relativa a las actividades realizadas de conformidad con sus responsabilidades establecidas en el presente Reglamento. Los Estados miembros concederán a las autoridades de control a que se refiere el artículo 51, apartado 1, del Reglamento (UE) 2016/679 acceso a sus registros contemplados en los artículos 10, 16, 24 y 36 del presente Reglamento, así como a la justificación a que se refiere el artículo 22, apartado 2 del presente Reglamento, y les permitirán acceder en todo momento a todos sus locales utilizados con fines de interoperabilidad.

Artículo 52

Auditorías por parte del Supervisor Europeo de Protección de Datos

El Supervisor Europeo de Protección de Datos velará por que se lleve a cabo una auditoría de las operaciones de tratamiento de datos realizadas por eu-LISA, la unidad central SEIAV y Europol a efectos del presente Reglamento con arreglo a las normas internacionales de auditoría pertinentes, al menos cada cuatro años. Se enviará un informe de la auditoría al Parlamento Europeo, el Consejo, eu-LISA, la Comisión, los Estados miembros y la agencia de la Unión de que se trate. Se brindará a eu-LISA, a la unidad central SEIAV y a Europol la oportunidad de formular observaciones antes de la adopción de los informes.

eu-LISA, la unidad central SEIAV y Europol proporcionarán al Supervisor Europeo de Protección de Datos la información que les solicite, le dará acceso a todos los documentos y a los registros contemplados en los artículos 10, 16, 24 y 36 y le permitirán acceder a sus locales en todo momento.

Artículo 53

Cooperación entre las autoridades de control y el Supervisor Europeo de Protección de Datos

1. Las autoridades de control y el Supervisor Europeo de Protección de Datos, cada uno dentro del ámbito de sus competencias respectivas, cooperarán activamente en el marco de sus responsabilidades respectivas y garantizarán una supervisión coordinada del uso de los componentes de interoperabilidad y de la aplicación de otras disposiciones del presente Reglamento, en particular si el Supervisor Europeo de Protección de Datos o una autoridad nacional de control detectan discrepancias importantes entre las prácticas de los Estados miembros o transferencias potencialmente ilegales en la utilización de los canales de comunicación de los componentes de interoperabilidad.

2. En los casos contemplados en el apartado 1 del presente artículo, se velará por el control coordinado de conformidad con el artículo 62 del Reglamento (UE) 2018/1725.

3. El Comité Europeo de Protección de Datos remitirá un informe conjunto de sus actividades en virtud del presente artículo al Parlamento Europeo, el Consejo, la Comisión, Europol, la Agencia Europea de la Guardia de Fronteras y Costas y eu-LISA el 12 de junio de 2021 y cada dos años en lo sucesivo. Dicho informe incluirá un capítulo sobre cada Estado miembro, redactado por la autoridad de control del Estado miembro de que se trate.

CAPÍTULO VIII

Responsabilidades

Artículo 54

Responsabilidades de eu-LISA durante la fase de diseño y desarrollo

1. eu-LISA velará por que las infraestructuras centrales de los componentes de interoperabilidad funcionen de conformidad con el presente Reglamento.

2. Los componentes de interoperabilidad estarán alojados por eu-LISA en sus sitios técnicos y dispondrán de las funcionalidades establecidas en el presente Reglamento de conformidad con las condiciones de seguridad, disponibilidad, calidad y desempeño establecidas en el artículo 53, apartado 1.

3. eu-LISA será responsable del desarrollo de los componentes de interoperabilidad para todas las adaptaciones que exija la interoperabilidad de los sistemas centrales del SES, el VIS, el SEIAV, el SIS, Eurodac, el ECRIS-TCN, el PEB, el SCB compartido, el RCDI, el DIM y el RCIE.

Sin perjuicio del artículo 62, eu-LISA no tendrá acceso a ninguno de los datos personales tratados a través del PEB, el SCB compartido, el RCDI o el DIM.

eu-LISA definirá el diseño de la arquitectura física de los componentes de interoperabilidad, incluidas sus infraestructuras de comunicación y sus especificaciones técnicas, y su evolución en lo relativo a la infraestructura central y la infraestructura de comunicación segura, que será adoptado por el Consejo de Administración, previo dictamen favorable de la Comisión. eu-LISA realizará también cualquier adaptación necesaria del SIS, Eurodac o el ECRIS-TCN que se derive del establecimiento de la interoperatividad y que disponga el presente Reglamento.

eu-LISA desarrollará e implementará los componentes de interoperabilidad lo antes posible después de la entrada en vigor del presente Reglamento y la adopción por la Comisión de las medidas previstas en el artículo 8, apartado 2, el artículo 9, apartado 7, el artículo 28, apartados 5 y 6, el artículo 37, apartado 4, el artículo 38, apartado 4, el artículo 39, apartado 5, el artículo 43, apartado 5 y el artículo 74, apartado 10.

El desarrollo consistirá en la elaboración y aplicación de las especificaciones técnicas, los ensayos y la gestión y coordinación global del proyecto.

4. Durante la fase de diseño y desarrollo, se establecerá un comité de gestión del programa compuesto por un máximo de diez miembros. El comité estará compuesto por siete miembros designados por el Consejo de Administración de eu-LISA de entre sus miembros o sus suplentes, el presidente del grupo consultivo de interoperabilidad a que se refiere el artículo 71, un miembro representante de eu-LISA nombrado por su director ejecutivo y un miembro nombrado por la Comisión. Los miembros nombrados por el Consejo de Administración de eu-LISA solo podrán ser elegidos de entre los Estados miembros que estén plenamente obligados con arreglo al Derecho de la Unión por los instrumentos jurídicos reguladores del desarrollo, establecimiento, funcionamiento y uso de todos los sistemas de información de la Unión y que vayan a participar en los componentes de interoperabilidad.

5. El comité de gestión del programa se reunirá periódicamente y al menos tres veces por trimestre. Garantizará la gestión adecuada de la fase de diseño y desarrollo de los componentes de interoperabilidad.

El comité de gestión del programa presentará mensualmente al Consejo de Administración de eu-LISA informes por escrito sobre los progresos del proyecto. El comité de gestión del programa no tendrá competencias para adoptar decisiones ni mandato alguno de representación de los miembros del Consejo de Administración de eu-LISA.

6. El Consejo de Administración de eu-LISA establecerá el reglamento interno del comité de gestión del programa, que incluirá, en particular, normas relativas a:

a) la presidencia;

b) los lugares de reunión;

c) la preparación de las reuniones;

d) la admisión de expertos a las reuniones;

e) planes de comunicación que garanticen una información completa a los miembros del Consejo de Administración no participantes.

La presidencia la ostentará un Estado miembro que esté plenamente obligado con arreglo a el Derecho de la Unión por los instrumentos jurídicos reguladores del desarrollo, establecimiento, funcionamiento y uso de todos los sistemas de información de la UE y que vaya a participar en los componentes de interoperabilidad.

Todos los gastos de viaje y dietas de los miembros del comité de gestión del programa serán abonados por la agencia, y el artículo 10 del Reglamento interno de eu-LISA se aplicará mutatis mutandis. eu-LISA realizará las labores de secretaría del comité de gestión del programa.

El grupo consultivo de interoperabilidad a que se refiere el artículo 71 se reunirá periódicamente hasta que los componentes de interoperabilidad entren en funcionamiento. Presentará un informe al comité de gestión del programa después de cada una de sus reuniones. Asimismo, aportará los conocimientos técnicos para llevar a cabo las tareas del comité de gestión del programa y realizará un seguimiento del estado de preparación de los Estados miembros.

Artículo 55

Responsabilidades de eu-LISA tras la entrada en funcionamiento

1. Tras la entrada en funcionamiento de cada componente de interoperabilidad, eu-LISA será responsable de la gestión técnica de la infraestructura central de los componentes de interoperabilidad, incluidos el mantenimiento y los avances tecnológicos. En cooperación con los Estados miembros, garantizará que se utilice la mejor tecnología disponible sobre la base de un análisis coste-beneficio. eu-LISA también será responsable de la gestión técnica y la seguridad de la infraestructura de comunicación a que se refieren los artículos 6, 12, 17, 25 y 39.

La gestión técnica de los componentes de interoperabilidad consistirá en todas las tareas y soluciones técnicas necesarias para mantenerlos en funcionamiento y prestando servicio ininterrumpidamente a los Estados miembros y a las agencias de la Unión durante las veinticuatro horas del día, siete días a la semana, de conformidad con el presente Reglamento y, en particular, en el trabajo de mantenimiento y los desarrollos técnicos necesarios para garantizar que los componentes funcionen con una calidad técnica de un nivel satisfactorio, en particular en lo que se refiere al tiempo de respuesta para la consulta de las infraestructuras centrales, de acuerdo con las características técnicas.

Todos los componentes de interoperabilidad se desarrollarán y gestionarán de modo que se garanticen un acceso rápido, ininterrumpido, eficiente y controlado y la plena disponibilidad ininterrumpida de los componentes y de los datos almacenados en el DIM, en el SCB compartido y en el RCDI, así como un tiempo de respuesta acorde con las necesidades operativas de las autoridades de los Estados miembros y las agencias de la Unión.

2. Sin perjuicio del artículo 17 del Estatuto de los funcionarios de la Unión Europea, eu-LISA aplicará las normas adecuadas sobre secreto profesional u otras obligaciones de confidencialidad equivalentes a todos los miembros de su personal que deban trabajar con los datos almacenados en los componentes de interoperabilidad. Esta obligación seguirá siendo aplicable después de que dichos miembros del personal hayan cesado en el cargo o el empleo, o tras la terminación de sus actividades.

Sin perjuicio del artículo 62, la agencia no tendrá acceso a ninguno de los datos personales tratados a través del PEB, el SCB compartido, el RCDI y el DIM.

3. eu-LISA desarrollará y mantendrá un mecanismo y procedimientos para realizar controles de calidad de los datos almacenados en el SCB compartido y el RCDI de conformidad con el artículo 37.

4. eu-LISA desempeñará las funciones relativas a la formación sobre la utilización técnica de los componentes de interoperabilidad.

Artículo 56

Responsabilidades de los Estados miembros

1. Cada Estado miembro será responsable de:

a) la conexión con la infraestructura de comunicación del PEB y el RCDI;

b) la integración de los sistemas e infraestructuras nacionales existentes con el PEB, el RCDI y el DIM;

c) la organización, la gestión, el funcionamiento y el mantenimiento de su infraestructura nacional existente y su conexión con los componentes de interoperabilidad;

d) la gestión y las condiciones de acceso del personal debidamente autorizado de las autoridades nacionales competentes al PEB, el RCDI y el DIM, de conformidad con el presente Reglamento, y el establecimiento y la actualización periódica de la lista de dicho personal y sus perfiles;

e) la adopción de las medidas legislativas a que se refiere el artículo 20, apartados 5 y 6, para acceder al RCDI a efectos de identificación;

f) la verificación manual de diferentes identidades contemplada en el artículo 29;

g) el cumplimiento de los requisitos de calidad de los datos determinados con arreglo al Derecho de la Unión;

h) el pleno respeto de las normas de cada sistema de información de la UE, relativas a la seguridad e integridad de los datos personales;

i) la corrección de las deficiencias detectadas en el informe de valoración de la Comisión sobre la calidad de los datos a que se refiere el artículo 37, apartado 5.

2. Cada Estado miembro conectará a sus autoridades designadas con el RCDI.

Artículo 57

Responsabilidades de Europol

1. Europol garantizará el procesamiento de las consultas que se realicen por medio del PEB a los datos de Europol y adaptará en consecuencia su interfaz «Querying Europol Systems» (QUEST; consulta de los sistemas de Europol) para el nivel de protección básico (NPB) de datos.

2. Europol será responsable de la gestión de su personal debidamente autorizado y de la organización del uso y acceso de ese personal al PEB y el RCDI, de conformidad con el presente Reglamento, así como de la creación y actualización periódica de un listado de dicho personal y de sus perfiles.

Artículo 58

Responsabilidades de la unidad central SEIAV

La unidad central SEIAV será responsable de:

a) la verificación manual de identidades diferentes contemplada en el artículo 29;

b) la detección de identidades múltiples entre los datos almacenados en el SES, el VIS, Eurodac y el SIS, contemplada en el artículo 65.

CAPÍTULO IX

Modificaciones de otros instrumentos de la Unión

Artículo 59

Modificaciones del Reglamento (UE) 2018/1726

El Reglamento (UE) 2018/1726 se modifica como sigue:

1) El artículo 12 se sustituye por el texto siguiente:

«*Artículo 12*

Calidad de los datos

1. Sin perjuicio de la responsabilidad de los Estados miembros en relación con los datos introducidos en los sistemas cuyo funcionamiento es responsabilidad de eu-LISA, eu-LISA, en estrecha colaboración con sus grupos consultivos, establecerá, para todos los sistemas cuyo funcionamiento es responsabilidad de la Agencia, mecanismos y procedimientos automatizados de control de la calidad de los datos, indicadores comunes de calidad de los datos y normas de calidad mínimas relativas al almacenamiento de los datos, de conformidad con las disposiciones pertinentes de los instrumentos jurídicos de los sistemas del artículo 37 del Reglamento (UE) 2019/817 (*) y (UE) 2019/818 (**) del Parlamento Europeo y del Consejo.

2. eu-LISA establecerá un repositorio central, que contenga únicamente datos anonimizados, de informes y estadísticas de conformidad con el artículo 39 del Reglamento (UE) 2019/817 y (UE) 2019/818 sujeto a las disposiciones específicas de los instrumentos jurídicos que rigen el desarrollo, establecimiento, funcionamiento y uso de todos los sistemas informáticos de gran magnitud gestionados por la Agencia.

(*) Reglamento (UE) 2019/817 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de fronteras y visados y por el que se modifican los Reglamentos (CE) n.º 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 y (UE) 2018/1861 del Parlamento Europeo y del Consejo, y las Decisiones 2004/512/CE y 2008/633/JAI del Consejo (DO L 135 de 22.5.2019, p. 27).

(**) Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de cooperación policial y judicial, asilo y migración y por el que se modifica el Reglamento (UE) n.º 603/2013, el Reglamento (UE) 2018/1862, el Reglamento (UE) 2019/816 y el Reglamento (UE) 2018/1726 (DO L 135 de 22.5.2019, p. 85).».

2) El artículo 19, apartado 1, se modifica como sigue:

a) se añade la letra siguiente:

«ee *bis*) aprobar los informes sobre el estado actual de desarrollo de los componentes de interoperabilidad de conformidad con el artículo 78, apartado 2, del Reglamento (UE) 2019/817 y el artículo 74, apartado 4 del Reglamento (UE) 2019/818;»;

b) la letra ff) se sustituye por el texto siguiente:

«ff) aprobará los informes sobre el funcionamiento técnico del SIS II de conformidad con el artículo 60, apartado 7, del Reglamento (UE) 2018/1861 del Parlamento Europeo y del Consejo (*) y el artículo 74, apartado 8, del Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo (**); del VIS de conformidad con el artículo 50, apartado 3, del Reglamento (CE) n.º 767/2008 y el artículo 17, apartado 3, de la Decisión 2008/633/JAI; del SES de conformidad con el artículo 72, apartado 4, del Reglamento (UE) 2017/2226; del SEIAV de conformidad con el artículo 92, apartado 4, del Reglamento (UE) 2018/1240 sobre el ECRIS-TCN y la aplicación de referencia ECRIS de conformidad con el artículo 36, apartado 4, del Reglamento (UE) 2019/816 del Parlamento Europeo y del Consejo (***), y de los componentes de interoperabilidad de conformidad con el artículo 78, apartado 4, del Reglamento (UE) 2019/817 y el artículo 74, apartado 3 del Reglamento (UE) 2019/818;

(*) Reglamento (UE) 2018/1861 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de las inspecciones fronterizas, por el que se modifica el Convenio de aplicación del Acuerdo de Schengen y se modifica y deroga el Reglamento (CE) n.º 1987/2006 (DO L 312 de 7.12.2018, p. 14).

(**) Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y de la cooperación judicial en materia penal, por el que se modifica y deroga la Decisión 2007/533/JAI del Consejo, y se derogan el Reglamento (CE) n.º 1986/2006 del Parlamento Europeo y del Consejo y la Decisión 2010/261/UE de la Comisión (DO L 312 de 7.12.2018, p. 56).

(***) Reglamento (UE) 2019/816 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, por el que se establece un sistema centralizado para la identificación de los Estados miembros que poseen información sobre condenas de nacionales de terceros países y apátridas (ECRIS-NTP) a fin de complementar y apoyar el Sistema Europeo de Información de Antecedentes Penales y por el que se modifica el Reglamento (UE) 2018/1726 (DO L 135 de 22.5.2019, p. 1).»;

c) la letra hh) se sustituye por el texto siguiente:

«hh) aprobará observaciones formales sobre los informes de auditoría del Supervisor Europeo de Protección de datos con arreglo al artículo 56, apartado 2, del Reglamento (UE) 2018/1861; el artículo 42, apartado 2, del Reglamento (CE) n.º 767/2008; el artículo 31, apartado 2, del Reglamento (UE) n.º 603/2013; el artículo 56, apartado 2, del Reglamento (UE) 2017/2226; el artículo 67 del Reglamento (UE) 2018/1240; el artículo 29, apartado 2, del Reglamento (UE) 2019/816 del Parlamento Europeo y del Consejo, y el artículo 52 del Reglamento (UE) 2019/817 y (UE) 2019/818, y garantizará el seguimiento adecuado de dichas auditorías;»;

d) la letra mm) se sustituye por el texto siguiente:

«mm) garantizará la publicación anual de la lista de autoridades competentes autorizadas para la búsqueda directa de los datos incluidos en el SIS II con arreglo al artículo 41, apartado 8, del Reglamento (UE) 2018/1861 y al artículo 56, apartado 7, del Reglamento (UE) 2018/1862, junto con la lista de las oficinas de los sistemas nacionales del SIS II (oficinas N.SIS II) y las oficinas Sirene con arreglo al artículo 7, apartado 3, del Reglamento (UE) 2018/1861 y el artículo 7, apartado 3, del Reglamento (UE) 2018/1862, respectivamente, así como la lista de las autoridades competentes con arreglo al artículo 65, apartado 2, del Reglamento (UE) 2017/2226, la lista de las autoridades competentes con arreglo al artículo 87, apartado 2, del Reglamento (UE) 2018/1240 la lista de las autoridades competentes con arreglo al artículo 34 del Reglamento (UE) 2019/816 y la lista de las autoridades competentes con arreglo al artículo 71, apartado 1, del Reglamento (UE) 2019/817 y el artículo 67, apartado 1 del Reglamento (UE) 2019/818;».

3) En el artículo 22, el apartado 4 se sustituye por el texto siguiente:

«4. Europol y Eurojust podrán asistir a las reuniones del Consejo de Administración en calidad de observadores siempre que figure en el orden del día una cuestión relativa al SIS II relacionada con la aplicación de la Decisión 2007/533/JAI.

La Agencia Europea de la Guardia de Fronteras y Costas podrá asistir a las reuniones del Consejo de Administración en calidad de observadora siempre que figure en el orden del día una cuestión relativa al SIS en relación con la aplicación del Reglamento (UE) 2016/1624.

Europol también podrá asistir a las reuniones del Consejo de Administración en calidad de observador siempre que en el orden del día figure una cuestión relativa al VIS relacionada con la aplicación de la Decisión 2008/633/JAI o una cuestión relativa a Eurodac relacionada con la aplicación del Reglamento (UE) n.º 603/2013.

Europol también podrá asistir a las reuniones del Consejo de Administración en calidad de observador siempre que en el orden del día figure una cuestión relativa al SES en relación con la aplicación del Reglamento (UE) 2017/2226 o una cuestión relativa al SEIAV en relación con la aplicación del Reglamento (UE) 2018/1240.

La Agencia Europea de la Guardia de Fronteras y Costas también podrá asistir a las reuniones del Consejo de Administración en calidad de observadora cuando en el orden del día figure una cuestión relativa al SEIAV en relación con la aplicación del Reglamento (UE) 2018/1240.

Eurojust, Europol y la Fiscalía Europea también podrán asistir a las reuniones del Consejo de Administración en calidad de observadores siempre que en el orden del día figure una cuestión relativa al Reglamento (UE) 2019/816.

Europol, Eurojust y la Agencia Europea de la Guardia de Fronteras y Costas también podrán asistir a las reuniones del Consejo de Administración siempre que en el orden del día figure una cuestión relativa a los Reglamento (UE) 2019/817 y (UE) 2019/818.

El Consejo de Administración podrá invitar a cualquier otra persona, cuya opinión pueda ser de interés, a asistir a las reuniones en calidad de observador.».

4) En el artículo 24, apartado 3, la letra p) se sustituye por el texto siguiente:

«p) sin perjuicio del artículo 17 del Estatuto de los funcionarios, establecerá los requisitos de confidencialidad necesarios para atenerse a el artículo 17 del Reglamento (CE) n.º 1987/2006; el artículo 17 de la Decisión 2007/533/JAI; el artículo 26, apartado 9, del Reglamento (CE) n.º 767/2008; el artículo 4, apartado 4, del Reglamento (UE) n.º 603/2013; el artículo 37, apartado 4, del Reglamento (UE) 2017/2226; el artículo 74, apartado 2, del Reglamento (UE) 2018/1240; el artículo 11, apartado 16, del Reglamento (UE) 2019/816 y el artículo 55, apartado 2, del Reglamento (UE) 2019/817 y (UE) 2019/818.».

5) En el artículo 23, el apartado 3 se modifica como sigue:

a) en el apartado 1 se inserta la letra e *bis*) siguiente:

«e) el Grupo consultivo sobre interoperabilidad;»;

b) el apartado 3 se sustituye por el texto siguiente:

«3. Europol, Eurojust y la Agencia Europea de la Guardia de Fronteras y Costas designarán cada uno a un representante en el grupo consultivo del SIS II.

Europol podrá también designar a un representante en los grupos consultivos del VIS, Eurodac y el SES-SEIAV.

La Agencia Europea de la Guardia de Fronteras y Costas también podrá designar a un representante en el grupo consultivo SES-SEIAV.

Eurojust, Europol y la Fiscalía Europea podrán también designar a un representante en el grupo consultivo del ECRIS-TCN.

Europol, Eurojust y la Agencia Europea de la Guardia de Fronteras y Costas podrán también, cada uno de ellos, designar a un representante en el grupo consultivo de interoperabilidad.».

Artículo 60

Modificaciones del Reglamento (UE) 2018/1862

El Reglamento (UE) 2018/1862 queda modificado como sigue:

1) En el artículo 3, se añaden los puntos siguientes:

«18) "PEB": el portal europeo de búsqueda creado mediante el artículo 6, apartado 1, del Reglamento (UE) 2019/818 (*);

19) «SCB compartido»: el servicio de correspondencia biométrica compartido creado mediante el artículo 12, apartado 1, del Reglamento (UE) 2019/818;

20) «RCDI»: el registro común de datos de identidad creado mediante el artículo 17, apartado 1, del Reglamento (UE) 2019/818;

21) «DIM»: el detector de identidades múltiples creado mediante el artículo 25, apartado 1, del Reglamento (UE) 2019/818.

(*) Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, asilo y migración y por el que se modifican los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816 (DO L 135 de 22.5.2019, p. 85).».

2) El artículo 4 se modifica como sigue:

a) en el apartado 1, las letras b) y c) se sustituyen por el texto siguiente:

«b) un sistema nacional (N.SIS) en cada Estado miembro, compuesto por los sistemas de datos nacionales que se comunican con el SIS Central, y que incluirá al menos un N.SIS de respaldo nacional o compartido;

c) una infraestructura de comunicación entre la CS-SIS, la copia de seguridad de la CS-SIS y la NI-SIS (en lo sucesivo, "infraestructura de comunicación") que proporcione una red virtual codificada dedicada a los datos del SIS y al intercambio de datos entre las oficinas Sirene como dispone el artículo 7, apartado 2, y

d) una infraestructura de comunicación segura entre la CS-SIS y las infraestructuras centrales del PEB, el SCB compartido y el DIM;»;

b) se añaden los apartados siguientes:

«8. Sin perjuicio de los apartados 1 a 5, los datos del SIS sobre personas y documentos de viaje también podrán consultarse a través del PEB.

9. Sin perjuicio de los apartados 1 a 5 del presente artículo, los datos del SIS sobre personas y documentos de viaje también podrán transmitirse a través de la infraestructura de comunicación segura a que se refiere el apartado 1, letra e). Estas transmisiones solo podrán realizarse en la medida en que los datos sean necesarios para las funciones a que se refiere el Reglamento (UE) 2019/818.».

3) En el artículo 7, se inserta el apartado siguiente:

«2 *bis*. Las oficinas Sirene garantizarán asimismo la verificación manual de identidades diferentes, de conformidad con el artículo 29 del Reglamento (UE) 2019/818. En la medida en que sea necesario para llevar a cabo esta tarea, las oficinas Sirene tendrán acceso a la consulta de los datos almacenados en el RCDI y el DIM para los fines establecidos en los artículos 21 y 26 del Reglamento (UE) 2019/818.».

4) En el artículo 12, apartado 1, se inserta el párrafo siguiente:

«Los Estados miembros velarán por que todo acceso a datos personales a través del PEB también quede registrado, con el fin de que se pueda controlar la legalidad de la consulta, supervisar la legalidad del tratamiento de datos, proceder a un control interno y garantizar la integridad y seguridad de los datos.».

5) En el artículo 44, apartado 1, se añade la letra siguiente:

«f) comprobar diferentes identidades y luchar contra la usurpación de la identidad conforme a el capítulo V del Reglamento (UE) 2019/818.».

6) En el artículo 74, el apartado 7 se sustituye por el texto siguiente:

«7. A efectos del artículo 15, apartado 4, y de los apartados 3, 4 y 6 del presente artículo la Agencia almacenará los datos a que se refiere el artículo 15, apartado 4 y el apartado 3 del presente artículo, que no permitirán la identificación de los individuos en el repositorio central de informes y estadísticas a que se refiere el artículo 39 del Reglamento (UE) 2019/818.

eu-LISA autorizará a la Comisión y a los organismos a que se refiere el apartado 6 del presente artículo a obtener informes y estadísticas personalizadas. Previa solicitud, eu-LISA dará acceso al repositorio central para informes y estadísticas, de conformidad con el artículo 39 del Reglamento (UE) 2019/818, a los Estados miembros, la Comisión, Europol y la Agencia Europea de la Guardia de Fronteras y Costas.».

Artículo 61

Modificaciones del Reglamento (UE) 2019/816

El Reglamento (UE) 2019/816 queda modificado como sigue:

1) En el artículo 1, se añade la letra siguiente:

«c) las condiciones en las que el ECRIS-TCN contribuye a facilitar y ayudar a la identificación correcta de las personas registradas en este sistema, en las condiciones y para los objetivos finales mencionados en el artículo 20 del Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo (*), mediante el almacenamiento de datos sobre identidades, documentos de viaje y datos biométricos en el registro común de datos de identidad (RCDI).

(*) Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, asilo y migración y por el que se modifican los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816 (DO L 135 de 22.5.2019, p. 85).».

2) El artículo 2 se sustituye por el texto siguiente:

«*Artículo 2*

Ámbito de aplicación

El presente Reglamento se aplica al tratamiento de datos de identidad de los nacionales de terceros países que hayan sido objeto de condenas en los Estados miembros con el fin de identificar a los Estados miembros en los que se hayan pronunciado las condenas. A excepción del artículo 5, apartado 1, letra b) inciso ii), las disposiciones del presente Reglamento que se aplican a los nacionales de terceros países se aplican también a los ciudadanos de la Unión que tienen también la nacionalidad de un tercer país y que hayan sido objeto de condenas en los Estados miembros. El presente Reglamento también contribuye a facilitar y ayudar a la correcta identificación de las personas con arreglo al presente Reglamento y al Reglamento (UE) 2019/818.».

3) El artículo 3 se modifica como sigue:

a) se suprime el punto 8;

b) se añaden los puntos siguientes:

«19) "RCDI": el registro común de datos de identidad creado mediante el artículo 17, apartado 1, del Reglamento (UE) 2019/818;

20) "datos del ECRIS-TCN": todos los datos almacenados en el Sistema Central ECRIS-TCN y el RCDI, de conformidad con el artículo 5.

21) "PEB": el portal europeo de búsqueda establecido por el artículo 6, apartado 1, del Reglamento (UE) 2019/818».

4) El artículo 4, apartado 1, se modifica como sigue:

a) la letra a) se sustituye por el texto siguiente:

«a) un Sistema Central;»;

b) se inserta la letra siguiente:

«a *bis*) el RCDI»;

c) se añade la letra siguiente:

«e) una infraestructura de comunicación entre el sistema centralizado y las infraestructuras centrales del PEB y del RCDI.».

5) El artículo 5 se modifica como sigue:

a) en el apartado 1, la parte introductoria se sustituye por el texto siguiente:

«1. Para cada uno de los nacionales de terceros países condenados, la Autoridad central del Estado miembro que le condenó creará un registro de datos en ECRIS- TCN. El registro de datos incluirá:»;

b) se inserta el apartado siguiente:

«1 *bis*. El RCDI contendrá los datos a que se refiere apartado 1, letra b), y los siguientes datos del apartado 1, letra a): apellido(s); nombre(s) (de pila), fecha de nacimiento; lugar de nacimiento (ciudad y país); nacionalidad o nacionalidades; sexo; en su caso, los nombres anteriores y, cuando estén disponibles, seudónimos y alias; cuando estén disponibles, tipo y número del documento o documentos de viaje de la persona, así como el nombre de la autoridad responsable de su expedición. El RCDI puede contener los datos a que se refiere el artículo 5, apartado 3. Los demás datos ECRIS-TCN se almacenarán en el Sistema Central.».

6) En el artículo 8 se modifica como sigue:

a) el apartado 1 se sustituye por el texto siguiente:

«1. Los registros se conservarán en el sistema central y el RCDI durante el tiempo que los datos relativos a la condena o condenas de la persona en cuestión estén consignados en el registro de antecedentes penales.»;

b) el apartado 2 se sustituye por el texto siguiente:

«2. Al expirar el periodo de conservación a que se refiere el apartado 1, la autoridad central del Estado miembro de condena suprimirá sin demoras indebidas, del Sistema Central ECRIS-TCN y del RCDI, el registro de datos, incluidas las impresiones dactilares y las imágenes faciales. La supresión se hará automáticamente, en la medida de lo posible y, en cualquier caso, a más tardar un mes después de la expiración del periodo de conservación.».

7) El artículo 9, apartado 9 se modifica como sigue:

a) en el apartado 1, las palabras «el Sistema del ECRIS-TCN» se sustituyen por las palabras «el Sistema Central y el RCDI»;

b) en los apartados 2, 3 y 4, las palabras «el Sistema Central» se sustituyen por las palabras «el Sistema Central y el RCDI»;

8) En el artículo 10, apartado 1, se suprime la letra j).

9) En el artículo 12, apartado 2, las palabras «el Sistema Central» se sustituyen por las palabras «el Sistema Central y el RCDI».

10) En el artículo 13, apartado 2, las palabras «el Sistema Central» se sustituyen por las palabras «el Sistema Central y el RCDI».

11) En el artículo 23, apartado 2, las palabras «el Sistema Central» se sustituyen por las palabras «el Sistema Central y el RCDI».

12) El artículo 24 se modifica como sigue:

a) el apartado 1 se sustituye por el texto siguiente:

«1. Los datos incluidos en el Sistema Central del ECRIS-TCN y el RCDI serán tratados únicamente a efectos de la identificación de los Estados miembros que conservan información de antecedentes penales de nacionales de terceros países. Los datos incluidos en el RCDI se tratarán con arreglo al Reglamento (UE) 2019/818 para facilitar y agilizar la identificación correcta de las personas registradas en el ECRIS-TCN de conformidad con el presente Reglamento.»;

b) se añade el apartado siguiente:

«3. Sin perjuicio del apartado 2, el acceso a efectos de la consulta de los datos almacenados en el RCDI también estará reservado al personal debidamente autorizado de las autoridades nacionales de cada Estado miembro y al personal debidamente autorizado de las agencias de la Unión que sean competentes para los fines establecidos en el artículo 20 y el artículo 21 del Reglamento (UE) 2019/818. Este acceso se limitará a la medida en que los datos sean necesarios para la realización de sus tareas con arreglo a dichos fines, y será proporcionado a los objetivos perseguidos.».

13) En el artículo 32, el apartado 2 se sustituye por el texto siguiente:

«2. A los efectos del apartado 1 del presente artículo, eu-LISA almacenará los datos a los que se refiere el apartado 1 en el repositorio central de informes y estadísticas a que se refiere el artículo 39 del Reglamento (UE) 2019/818.».

14) En el artículo 33, apartado 1, las palabras «el Sistema Central» se sustituyen por las palabras «el Sistema Central, el RCDI y».

15) En el artículo 41, el apartado 2 se sustituye por el texto siguiente:

«2. Para condenas pronunciadas antes de la fecha de introducción de los datos de acuerdo con el artículo 35, apartado 1, las autoridades centrales crearán los registros de datos individuales en el sistema central y en el RCDI de la siguiente forma:

a) los datos alfanuméricos se introducirán en el sistema central y en el RCDI al final del período a que se refiere el artículo 35, apartado 2;

b) los datos dactiloscópicos se introducirán en el sistema central y en el RCDI dos años después del comienzo del funcionamiento, de conformidad con el artículo 35, apartado 4».

CAPÍTULO X

Disposiciones finales

Artículo 62

Presentación de informes y estadísticas

1. El personal debidamente autorizado de las autoridades competentes de los Estados miembros, la Comisión y eu-LISA tendrán acceso a consultar, únicamente a efectos de la presentación de informes y estadísticas, el número de consultas por usuario del perfil del PEB.

No será posible identificar individuos a partir de los datos.

2. El personal debidamente autorizado de las autoridades competentes de los Estados miembros, la Comisión y eu-LISA tendrá acceso a la consulta de los datos siguientes en relación con el RCDI, únicamente a efectos de la presentación de informes y estadísticas:

a) número de consultas a los efectos de los artículos 20, 21 y 22;

b) nacionalidad, género y año de nacimiento de la persona;

c) tipo de documento de viaje y código de tres letras del país de expedición;

d) número de búsquedas realizadas con y sin datos biométricos.

No será posible identificar individuos a partir de los datos.

3. El personal debidamente autorizado de las autoridades competentes de los Estados miembros, la Comisión y eu-LISA tendrá acceso a la consulta de los datos siguientes en relación con el DIM, únicamente a efectos de la presentación de informes y estadísticas y sin que ello le otorgue competencias para la identificación individual:

a) número de búsquedas realizadas con y sin datos biométricos;

b) número de cada tipo de vínculo y los sistemas de información de la UE que contienen datos vinculados;

c) periodo durante el que se ha mantenido un vínculo amarillo o rojo en el sistema.

No será posible identificar individuos a partir de los datos.

4. El personal debidamente autorizado de la Agencia Europea de la Guardia de Fronteras y Costas tendrá acceso a la consulta de los datos a que se refieren los apartados 1, 2 y 3 del presente artículo con el fin de llevar a cabo los análisis de riesgos y la evaluación de la vulnerabilidad a que se hace referencia en los artículos 11 y 13 del Reglamento (UE) 2016/1624 del Parlamento Europeo y del Consejo ([38]).

5. El personal debidamente autorizado de Europol tendrá acceso a la consulta de los datos a que se refieren los apartados 2 y 3 del presente artículo con el fin de llevar a cabo los análisis estratégicos, temáticos y operativos a que se hace referencia en el artículo 18, apartado 2, letras b) y c), del Reglamento (UE) 2016/794.

6. A los efectos de los apartados 1, 2 y 3 del presente artículo, eu-LISA almacenará los datos a los que se refieren dichos apartados en el RCIE. No será posible identificar individuos a partir de los datos contenidos en el RCIE, pero los datos permitirán a las autoridades enumeradas en los apartados 1, 2 y 3 la elaboración de informes y estadísticas personalizados para mejorar la eficiencia de los controles fronterizos, para ayudar a las autoridades a tramitar las solicitudes de visado y para respaldar la elaboración de políticas basadas en pruebas en el ámbito de la migración y la seguridad en la Unión.

7. Previa solicitud, la Comisión pondrá a disposición de la Agencia de los Derechos Fundamentales de la Unión Europea la información pertinente a fin de evaluar las repercusiones del presente Reglamento en los derechos fundamentales.

([38]) Reglamento (UE) 2016/1624 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2016, sobre la Guardia Europea de Fronteras y Costas, por el que se modifica el Reglamento (UE) 2016/399 del Parlamento Europeo y del Consejo y por el que se derogan el Reglamento (CE) n.º 863/2007 del Parlamento Europeo y del Consejo, el Reglamento (CE) n.º 2007/2004 del Consejo y la Decisión 2005/267/CE del Consejo (DO L 251 de 16.9.2016, p. 1).

Artículo 63

Periodo transitorio para la utilización del portal europeo de búsqueda

1. Durante un periodo de dos años a partir de la fecha en que el PEB entre en funcionamiento, no serán de aplicación las obligaciones a que se refiere el artículo 7, apartados 2 y 4, y la utilización del PEB será facultativa.

2. La Comisión estará facultada para adoptar actos delegados, con arreglo al artículo 69 a fin de modificar el presente Reglamento prorrogando una vez el periodo a que se hace referencia en el apartado 1 del presente artículo por un periodo no superior a un año si una evaluación de la aplicación práctica del PEB muestra que es necesaria tal prórroga especialmente debido a las repercusiones de la introducción del PEB en la organización y la duración de los controles fronterizos.

Artículo 64

Periodo transitorio aplicable a las disposiciones sobre el acceso al registro común de datos de identidad con fines de prevención, detección o investigación de delitos de terrorismo u otros delitos graves

El artículo 22 será de aplicación a partir de la fecha de entrada en funcionamiento del RCDI a que se refiere el artículo 68, apartado 3.

Artículo 65

Periodo transitorio para el detector de identidades múltiples

1. Durante un periodo de un año tras la notificación por parte de eu-LISA de la realización del ensayo al que se hace referencia en el artículo 68, apartado 4, letra b), relativo al DIM y antes de la entrada en funcionamiento del DIM, la unidad central SEIAV a que se refiere el artículo 33, letra a), del Reglamento (UE) 2016/1624 se encargará de efectuar una detección de identidades múltiples entre los datos almacenados en el SES, el VIS, Eurodac y el SIS. Las detecciones de identidades múltiples se llevarán a cabo utilizando solamente datos biométricos, de conformidad con el artículo 27, apartado 2, del presente Reglamento.

2. Cuando la consulta dé lugar a una o varias correspondencias y los datos de identidad de los expedientes vinculados sean los mismos o similares, se creará un vínculo blanco de conformidad con el artículo 33.

Cuando la consulta dé lugar a una o varias correspondencias y los datos de identidad de los expedientes vinculados no puedan considerarse similares, se creará un vínculo amarillo de conformidad con el artículo 30 y será de aplicación el procedimiento a que se refiere el artículo 29.

Cuando se registren varias correspondencias, se creará un vínculo a cada uno de los datos que hayan dado lugar a una correspondencia.

3. Cuando se cree un vínculo amarillo, el DIM concederá a la unidad central SEIAV acceso a los datos de identidad presentes en los distintos sistemas de información.

4. Cuando se cree un vínculo a una descripción en el SIS, distinta de una descripción de denegación de entrada o retorno o una descripción relativa a un documento de viaje declarado perdido, robado o invalidado de conformidad con el artículo 3 del Reglamento (UE) 2018/1860, los artículos 24 y 25 del Reglamento (UE) 2018/1861 y el artículo 38 del Reglamento (UE) 2018/1862 respectivamente, el DIM concederá a la oficina Sirene del Estado miembro que haya creado la descripción acceso a los datos de identidad presentes en los distintos sistemas de información.

5. La unidad central SEIAV o la oficina Sirene del Estado miembro que haya creado la descripción tendrán acceso a los datos contenidos en el expediente de confirmación de identidad, evaluarán las diferentes identidades y actualizarán el vínculo con arreglo a los artículos 31, 32 y 33 y lo añadirán al expediente de confirmación de identidad.

6. La unidad central SEIAV notificará a la Comisión de conformidad con el artículo 67, apartado 3, únicamente una vez que se hayan verificado todos los vínculos amarillos y se hayan actualizado como vínculos verdes, blancos o rojos.

7. Los Estados miembros prestarán asistencia, cuando sea necesario, a la unidad central SEIAV en la detección de identidades múltiples a que se refiere el presente artículo.

8. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 69 a fin de prorrogar el periodo a que se refiere el apartado 1 por seis meses, renovables dos veces por seis meses cada vez. Esta prórroga se concederá únicamente si una evaluación del tiempo estimado para la finalización de la detección de identidades múltiples a que se hace referencia en el presente artículo, que demuestre que la detección de identidades múltiples no se puede llevar a cabo antes del vencimiento de la fecha límite a que se hace referencia en el apartado 1 del presente artículo o de la fecha de las dos primeras prórrogas, por razones ajenas a la unidad central SEIAV y que no pueden aplicarse medidas de corrección. La evaluación se llevará a cabo a más tardar tres meses antes de la expiración de dicho período o la prórroga vigente del mismo.

Artículo 66

Costes

1. Los costes en que se incurra en relación con la creación y funcionamiento del PEB, el SCB compartido, el RCDI y el DIM correrán a cargo del presupuesto general de la Unión.

2. Los costes en que se incurra en relación con la integración de las infraestructuras nacionales existentes y su conexión a las interfaces nacionales uniformes, así como en relación con el alojamiento de las interfaces nacionales uniformes, correrán a cargo del presupuesto general de la Unión.

Quedan excluidos los costes siguientes:

a) la oficina de gestión del proyecto de los Estados miembros (reuniones, misiones, despachos);

b) el alojamiento de los sistemas informáticos nacionales (espacio, ejecución, electricidad, refrigeración);

c) el funcionamiento de los sistemas informáticos nacionales (operadores y contratos de apoyo);

d) el diseño, el desarrollo, la implementación, la explotación y el mantenimiento de las redes de comunicación nacionales.

3. Sin perjuicio de que se destinen más fondos a este propósito a partir de otras fuentes del presupuesto general de la Unión, se movilizará un importe de 32 077 000 EUR de la partida de 791 000 000 EUR prevista en el artículo 5, apartado 5, letra b), del Reglamento (UE) n.º 515/2014 para cubrir los costes de aplicación del presente Reglamento, según lo previsto en los apartados 1 y 2 del presente artículo.

4. De la partida mencionada en el apartado 3, 22 861 000 EUR se asignarán a eu-LISA, 9 072 000 se asignarán a Europol y 144 000 EUR, a la Agencia de la Unión Europea para la Formación Policial (CEPOL) con miras a brindar apoyo a estas agencias en la ejecución de sus tareas respectivas en consonancia con los requisitos del presente Reglamento. Tal financiación se ejecutará en régimen de gestión indirecta.

5. Los costes en que incurran las autoridades designadas correrán a cargo del Estado miembro que las designe, respectivamente. Los costes generados por la conexión de las autoridades designadas al RCDI correrán a cargo de cada Estado miembro.

Los costes en que incurra Europol, incluida la conexión al RCDI, correrán a cargo de Europol.

Artículo 67

Notificaciones

1. Los Estados miembros notificarán a eu-LISA las autoridades a que se refieren los artículos 7, 20, 21 y 26 que podrán utilizar el PEB, el RCDI y el DIM o tener acceso a ellos, respectivamente.

La lista consolidada de dichas autoridades se publicará en el *Diario Oficial de la Unión Europea* en un plazo de tres meses a partir de la fecha en que cada componente de interoperabilidad entre en funcionamiento, de conformidad con el artículo 68. Cuando se modifique dicha lista, eu-LISA publicará una lista consolidada actualizada una vez al año.

2. eu-LISA notificará a la Comisión la realización satisfactoria de los ensayos mencionados en el artículo 68, letras b), de los apartados 1 a 6.

3. eu-LISA notificará a la Comisión la realización satisfactoria de la medida transitoria establecida en el artículo 65.

4. La Comisión pondrá a disposición de los Estados miembros y del público, mediante un sitio web público constantemente actualizado, la información notificada de conformidad con el apartado 1.

Artículo 68

Entrada en funcionamiento

1. La Comisión determinará la fecha a partir de la que el PEB debe entrar en funcionamiento, mediante un acto de ejecución y una vez que se cumplan las condiciones siguientes:

a) que se hayan adoptado las medidas a que se refieren el artículo 8, apartado 2; el artículo 9, apartado 7, y el artículo 43, apartado 5;

b) que eu-LISA haya declarado la realización satisfactoria de un ensayo global del PEB, que eu-LISA debe llevar a cabo en cooperación con los Estados miembros y las agencias de la Unión que pueden utilizar el PEB;

c) que eu-LISA haya validado las disposiciones legales y técnicas necesarias para recoger y transmitir los datos a que se refiere el artículo 8, apartado 1, y las haya notificado a la Comisión.

El PEB solo podrá consultar las bases de datos de Interpol cuando las disposiciones técnicas permitan cumplir con el artículo 9, apartado 5. La imposibilidad de cumplir con el artículo 9, apartado 5 tendrá como resultado que el PEB no consulte las bases de datos de Interpol, pero no retrasará la entrada en funcionamiento del PEB.

La Comisión establecerá que la fecha a que se refiere el párrafo primero sea en un plazo de treinta días a partir de la adopción del acto de ejecución.

2. La Comisión determinará la fecha a partir de la que el SCB compartido debe entrar en funcionamiento, mediante un acto de ejecución y una vez que se cumplan las condiciones siguientes:

a) que se hayan adoptado las medidas contempladas en el artículo 13, apartado 5, y en el artículo 43, apartado 5;

b) que eu-LISA haya declarado la realización satisfactoria de un ensayo global del SCB compartido, que ha llevado a cabo en cooperación con las autoridades de los Estados miembros;

c) que eu-LISA haya validado las disposiciones legales y técnicas necesarias para recoger y transmitir los datos a que se refieren el artículo 13 y las haya notificado a la Comisión;

d) que eu-LISA haya declarado la realización satisfactoria del ensayo mencionado en el apartado 1 *quinquies*, letra b).

La Comisión establecerá que la fecha a que se refiere el párrafo primero sea en un plazo de treinta días a partir de la adopción del acto de ejecución.

3. La Comisión determinará la fecha a partir de la que el RCDI debe entrar en funcionamiento, mediante un acto de ejecución y una vez que se cumplan las condiciones siguientes:

a) que se hayan adoptado las medidas contempladas en el artículo 43, apartado 5, y en el artículo 74, apartado 10;

b) que eu-LISA haya declarado la realización satisfactoria de un ensayo global del RCDI, que ha llevado a cabo en cooperación con las autoridades de los Estados miembros;

c) que eu-LISA haya validado las disposiciones legales y técnicas necesarias para recoger y transmitir los datos a que se refiere el artículo 18 y las haya notificado a la Comisión;

d) que eu-LISA haya declarado la realización satisfactoria del ensayo mencionado en el apartado 1 *quinquies*, letra b).

La Comisión establecerá que la fecha a que se refiere el párrafo primero sea en un plazo de treinta días a partir de la adopción del acto de ejecución.

4. La Comisión determinará la fecha a partir de la que el DIM debe entrar en funcionamiento, mediante un acto de ejecución y una vez que se cumplan las condiciones siguientes:

a) que se hayan adoptado las medidas a que se refieren el artículo 28, apartados 5 y 7, el artículo 32, apartado 5, el artículo 33, apartado 6, el artículo 43, apartado 5, y el artículo 49, apartado 6;

b) que eu-LISA haya declarado la realización satisfactoria de un ensayo global del DIM, que ha llevado a cabo en cooperación con las autoridades de los Estados miembros y la unidad central SEIAV;

c) que eu-LISA haya validado las disposiciones legales y técnicas necesarias para recoger y transmitir los datos a que se refiere el artículo 34 y las haya notificado a la Comisión;

d) que la unidad central SEIAV haya notificado a la Comisión de acuerdo con el artículo 67, apartado 3, a la Comisión;

e) que eu-LISA haya declarado la realización satisfactoria de los ensayos mencionados en los apartados 1, letra b), 2, letra b), 3, letra b), y 5, letra b).

La Comisión establecerá que la fecha a que se refiere el párrafo primero sea en un plazo de treinta días a partir de la adopción del acto de ejecución.

5. La Comisión establecerá mediante un acto de ejecución la fecha a partir de la que deben utilizarse los mecanismos y procedimientos automatizados de control de calidad de los datos, los indicadores comunes de calidad de los datos y las normas mínimas de calidad de los datos, una vez que se hayan cumplido las condiciones siguientes:

a) que se hayan adoptado las medidas a que se refiere el artículo 37, apartado 4;

b) que eu-LISA haya declarado la realización satisfactoria de un ensayo global de los mecanismos y procedimientos automatizados de control de calidad de los datos, los indicadores comunes de calidad de los datos y las normas mínimas de calidad de los datos, que eu-LISA ha llevado a cabo en cooperación con las autoridades de los Estados miembros.

La Comisión establecerá que la fecha a que se refiere el párrafo primero sea en un plazo de treinta días a partir de la adopción del acto de ejecución.

6. La Comisión determinará la fecha a partir de la que el RCIE debe entrar en funcionamiento, mediante un acto de ejecución y una vez que se hayan cumplido las condiciones siguientes:

a) que se hayan adoptado las medidas a que se refieren el artículo 39, apartado 5, y el artículo 44, apartado 5;

b) que eu-LISA haya declarado la realización satisfactoria de un ensayo global del RCIE, que ha llevado a cabo en cooperación con las autoridades de los Estados miembros;

c) que eu-LISA haya validado las disposiciones legales y técnicas necesarias para recoger y transmitir los datos a que se refiere el artículo 39 y las haya notificado a la Comisión.

La Comisión establecerá que la fecha a que se refiere el párrafo primero sea en un plazo de treinta días a partir de la adopción del acto de ejecución.

7. La Comisión informará al Parlamento Europeo y al Consejo de los resultados del ensayo realizado de conformidad con las letras b) de los apartados 1 a 6.

8. Los Estados miembros, la unidad central SEIAV y Europol comenzarán a utilizar cada uno de los componentes de interoperabilidad a partir de la fecha determinada por la Comisión de conformidad con los apartados 1, 2, 3 y 4 respectivamente.

Artículo 69

Ejercicio de la delegación

1. Se otorgan a la Comisión los poderes para adoptar actos delegados en las condiciones establecidas en el presente artículo.

2. Los poderes para adoptar los actos delegados mencionados en el artículo 28, apartado 5, en el artículo 39, apartado 5, en el artículo 49, apartado 6, en el artículo 63, apartado 2, y en el artículo 65, apartado 8, se otorgan a la Comisión por un periodo de cinco años a partir del 11 de junio de 2019. La Comisión elaborará un informe sobre la delegación de poderes a más tardar nueve meses antes de que finalice el periodo de cinco años. La delegación de poderes se prorrogará tácitamente por periodos de idéntica duración, excepto si el Parlamento Europeo o el Consejo se oponen a dicha prórroga a más tardar tres meses antes del final de cada periodo.

3. La delegación de poderes mencionada en el artículo 28, apartado 5, en el artículo 39, apartado 5, en el artículo 49, apartado 6, en el artículo 63, apartado 2, y en el artículo 65, apartado 8, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto al día siguiente de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior indicada en la misma. No afectará a la validez de los actos delegados que ya estén en vigor.

4. Antes de la adopción de un acto delegado, la Comisión consultará a los expertos designados por cada Estado miembro de conformidad con los principios establecidos en el Acuerdo interinstitucional sobre la mejora de la legislación de 13 de abril de 2016.

5. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.

6. Los actos delegados adoptados en virtud de los artículos 28, apartado 5, 39, apartado 5, 49, apartado 6, 63, apartado 2, y 65, apartado 8, entrarán en vigor únicamente si, en un plazo de dos meses desde su notificación al Parlamento Europeo y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no las formularán. El plazo se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 70

Procedimiento de comité

1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.

2. En los casos en que se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.

Si el comité no emite un dictamen, la Comisión no adoptará el proyecto de acto de ejecución y se aplicará el artículo 5, apartado 4, párrafo tercero, del Reglamento (UE) n.º 182/2011.

Artículo 71

Grupo consultivo

eu-LISA creará un grupo consultivo de interoperabilidad. Durante la fase de diseño y desarrollo de los componentes de interoperabilidad, se aplicará el artículo 54, apartados 4, 5 y 6.

Artículo 72

Formación

eu-LISA desempeñará las funciones relacionadas con la formación sobre el uso técnico de los componentes de interoperabilidad, de conformidad con el Reglamento (UE) n.º 1077/2011.

Las autoridades de los Estados miembros y las agencias de la Unión proporcionarán a su personal autorizado a usar los datos de los componentes de interoperabilidad programas de formación adecuados sobre seguridad de datos, calidad de datos, normas de protección de datos, procedimientos aplicables al tratamiento de datos y la obligación de informar con arreglo a los artículos 32, apartado 4, 33, apartado 4 y 47.

Cuando proceda, se organizarán cursos de formación comunes sobre estos temas a escala de la Unión para reforzar la cooperación y el intercambio de las mejores prácticas entre el personal de los Estados miembros y las agencias de la Unión autorizadas a tratar datos de los componentes de interoperabilidad. Debe prestarse especial atención al proceso de detección de identidades múltiples, incluida la verificación manual de identidades diferentes y la necesidad concomitante de mantener salvaguardias apropiadas de los derechos fundamentales.

Artículo 73

Manual práctico

La Comisión, en estrecha cooperación con los Estados miembros, eu-LISA y otras agencias pertinentes de la Unión, publicará un manual práctico de aplicación y gestión de los componentes de interoperabilidad. El manual práctico proporcionará orientaciones técnicas y operativas, recomendaciones y mejores prácticas. La Comisión adoptará el manual práctico en forma de recomendación.

Artículo 74

Supervisión y valoración

1. eu-LISA se asegurará de que se establezcan procedimientos para llevar a cabo la supervisión del desarrollo de los componentes de interoperabilidad y de su conexión a la interfaz nacional uniforme a la luz de los objetivos en materia de planificación y costes, y de su funcionamiento a la luz de los objetivos en materia de resultados técnicos, rentabilidad, seguridad y calidad del servicio.

2. A más tardar el 12 de diciembre de 2019, y posteriormente cada seis meses durante la fase de desarrollo de los componentes de interoperabilidad, eu-LISA presentará un informe al Parlamento Europeo y al Consejo sobre el estado de desarrollo de los componentes de interoperabilidad y de su conexión a la interfaz nacional uniforme. Una vez finalizado el desarrollo, se presentará un informe al Parlamento Europeo y al Consejo en el que se explique con detalle cómo se han conseguido los objetivos, en particular en lo relativo a la planificación y los costes, y se justifique toda divergencia.

3. Cuatro años después de la entrada en funcionamiento de cada componente de interoperabilidad de conformidad con el artículo 68 y, posteriormente, cada cuatro años, eu-LISA presentará al Parlamento Europeo, al Consejo y a la Comisión un informe sobre el funcionamiento técnico de los componentes de interoperabilidad, incluida su seguridad.

4. Además, un año después de cada informe de eu-LISA, la Comisión realizará una valoración global de los componentes de interoperabilidad, que incluirá:

a) una evaluación de la aplicación del presente Reglamento;

b) un examen de los resultados alcanzados en comparación con los objetivos del presente Reglamento y de su repercusión sobre los derechos fundamentales, en particular sobre los efectos de los componentes de interoperabilidad para el derecho a la no discriminación;

c) una evaluación del funcionamiento del portal web, incluidas las cifras relativas al uso del portal web y el número de solicitudes resueltas;

d) una evaluación de la vigencia de los motivos que fundamentan los componentes de interoperabilidad;

e) una evaluación de la seguridad de los componentes de interoperabilidad;

f) una evaluación del uso del RCDI con fines de identificación;

g) una evaluación del uso del RCDI con fines de prevención, detección o investigación de delitos de terrorismo u otros delitos graves;

h) una evaluación de las consecuencias, incluida cualquier repercusión desproporcionada, en el flujo de tráfico en los pasos fronterizos y de aquellas consecuencias que tengan incidencia en el presupuesto de la Unión;

i) una evaluación de la búsqueda en bases de datos de Interpol a través del PEB, con información sobre el número de correspondencias obtenidas con las bases de datos de Interpol y sobre los problemas detectados.

Las valoraciones globales incluirán todas las recomendaciones necesarias. La Comisión remitirá el informe de valoración al Parlamento Europeo, al Consejo, al Supervisor Europeo de Protección de Datos y a la Agencia de los Derechos Fundamentales de la Unión Europea.

5. A más tardar el 12 de junio de 2020 y posteriormente cada año hasta que se adopten los actos de ejecución de la Comisión a que se refiere el artículo 68, la Comisión presentará un informe al Parlamento Europeo y al Consejo sobre el estado de los preparativos para la plena aplicación del presente Reglamento. Dicho informe contendrá también información pormenorizada sobre los costes soportados y sobre los riesgos que puedan afectar a los costes globales.

6. Dos años después de que entre en funcionamiento el DIM de conformidad con el artículo 68, apartado 4, la Comisión llevará a cabo un examen de los efectos del DIM sobre el derecho a la no discriminación dos años después de que el DIM entre en funcionamiento. Tras este primer informe, el examen de los efectos del DIM sobre el derecho a la no discriminación formará parte del examen a que se hace referencia en el apartado 4, letra b) del presente artículo.

7. Los Estados miembros y Europol proporcionarán a eu-LISA y a la Comisión la información necesaria para elaborar los informes a que se refieren los apartados 3 a 6. Esta información no deberá nunca poner en riesgo los métodos de trabajo ni incluir datos que revelen fuentes, miembros del personal o investigaciones de las autoridades designadas.

8. eu-LISA facilitará a la Comisión la información necesaria para realizar las valoraciones a que se refiere el apartado 4.

9. Con pleno respeto de las disposiciones del Derecho nacional en materia de publicación de información sensible y sin perjuicio de las limitaciones necesarias para proteger la seguridad y el orden público, prevenir la delincuencia y garantizar que ninguna investigación nacional corra peligro, cada Estado miembro y Europol prepararán informes anuales sobre la eficacia del acceso a los datos almacenados en el RCDI con fines de prevención, detección o investigación de los delitos de terrorismo u otros delitos graves, que comprenderán información y estadísticas sobre:

a) la finalidad exacta de la consulta, incluido el tipo de delito de terrorismo u otros delitos graves;

b) los motivos razonables alegados para la sospecha fundada de que el sospechoso, el autor o la víctima están cubiertos por el Reglamento (UE) n.º 603/2013;

c) el número de solicitudes de acceso al RCDI con fines de prevención, detección o investigación de delitos de terrorismo o de otros delitos graves;

d) el número y tipo de casos que hayan arrojado identificaciones positivas;

e) la necesidad y la utilización del recurso excepcional de urgencia, incluyendo aquellos casos en los que la urgencia no fue aceptada por la verificación efectuada a posteriori por el punto de acceso central.

Los informes anuales de los Estados miembros y de Europol se remitirán a la Comisión antes del 30 de junio del año siguiente.

10. Se pondrá a disposición de los Estados miembros una solución técnica con el fin de gestionar las solicitudes de acceso de los usuarios a que se hace referencia en el artículo 22 y de facilitar la recopilación de información con arreglo a los apartados 7 y 9 del presente artículo a efectos de la generación de informes y estadísticas contemplados en dichos apartados. La Comisión adoptará actos de ejecución para establecer las especificaciones de las soluciones técnicas. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 70, apartado 2.

Artículo 75

Entrada en vigor y aplicación

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

Las disposiciones del presente Reglamento en relación con el PEB, se aplicarán a partir de la fecha determinada por la Comisión de conformidad con el artículo 68, apartado 1.

Las disposiciones del presente Reglamento en relación con el SCB compartido se aplicarán a partir de la fecha determinada por la Comisión de conformidad con el artículo 68, apartado 2.

Las disposiciones del presente Reglamento en relación con el RCDI se aplicarán a partir de la fecha determinada por la Comisión de conformidad con el artículo 68, apartado 3.

Las disposiciones del presente Reglamento en relación con el DIM se aplicarán a partir de la fecha determinada por la Comisión de conformidad con el artículo 68, apartado 4.

Las disposiciones del presente Reglamento relativas a los mecanismos y procedimientos automatizados de control de calidad de los datos, los indicadores comunes de calidad de los datos y las normas mínimas de calidad se aplicarán a partir de la fecha determinada por la Comisión de conformidad con el artículo 68, apartado 5.

Las disposiciones del presente Reglamento relativas al RCIE se aplicarán a partir de la fecha determinada por la Comisión de conformidad con el artículo 68, apartado 6.

Los artículos 6, 12, 17, 25, 38, 42, 54, 56, 58, 66, 67, 69, 70, 71, 73 y 74, apartado 1, se aplicarán a partir del 11 de junio de 2019.

El presente Reglamento se aplicará respecto de Eurodac a partir de la fecha en que sea aplicable el texto refundido del Reglamento (UE) n.º 603/2013.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en los Estados miembros de conformidad con los Tratados.

Hecho en Bruselas, el 20 de mayo de 2019.

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente*
A. TAJANI	G. CIAMBA